Panduan Referensi

AWS Kebijakan Terkelola

AWS Kebijakan Terkelola: Panduan Referensi

Table of Contents

Apa itu kebijakan yang AWS dikelola?

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola olehAWS. AWSkebijakan terkelola dirancang untuk memberikan izin untuk banyak kasus penggunaan umum. Mereka memudahkan Anda untuk memulai dengan menetapkan izin kepada pengguna, grup, dan peran daripada jika Anda harus menulis kebijakan sendiri.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan oleh semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan yang dikelola AWS. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pemutakhiran akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWSkemungkinan besar akan memperbarui kebijakan AWS terkelola saat AWS layanan baru diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat kebijakan AWS terkelola di Panduan Pengguna IAM.

Memahami halaman referensi kebijakan

Setiap halaman referensi kebijakan mencakup informasi berikut:

- Menggunakan kebijakan ini — Apakah Anda dapat melampirkan kebijakan ke pengguna, grup, dan peran
- Rincian kebijakan
  - Jenis — Jenis kebijakan AWS terkelola
    - `AWS managed policy`— Kebijakan AWS terkelola standar
    - `Job function policy`— Kebijakan yang sejalan dengan fungsi pekerjaan industri umum
    - `Service-linked role policy`Kebijakan yang dilampirkan pada peran terkait layanan yang memungkinkan layanan untuk melakukan tindakan atas nama Anda, seperti the section called “AmazonRDSPreviewServiceRolePolicy”
    - `Service role policy`— Kebijakan yang dirancang untuk bekerja dengan peran layanan, seperti the section called “AWSControlTowerServiceRolePolicy”
  - Waktu pembuatan — Saat kebijakan pertama kali dibuat

  - Waktu yang diedit - Saat versi kebijakan ini diedit
  - ARN - Nama Sumber Daya Amazon dari kebijakan
- Versi kebijakan — Versi izin yang diberikan oleh kebijakan
- Dokumen kebijakan JSON — Kebijakan JSON
- Pelajari selengkapnya - Tautan ke dokumentasi yang terkait dengan kebijakan AWS terkelola

Kebijakan terkelola AWS tidak lagi digunakan

AWSmemperbarui kebijakan AWS terkelola secara berkala. Dalam kebanyakan kasus, kami menambahkan izin ke kebijakan. Ini terjadi ketika kami meluncurkan layanan atau fitur baru. Untuk meningkatkan keamanan kebijakan yang AWS dikelola, terkadang kami mengurangi ruang lingkup kebijakan. Saat kami menghapus izin dari kebijakan, kami menetapkan kebijakan ke status usang dan membuat yang baru tersedia. Saat AWS menghentikan layanan atau fitur, kami juga menghentikan kebijakan terkelola untuk fitur tersebut. AWS

Jika Anda menerima pemberitahuan email bahwa kebijakan yang Anda gunakan tidak berlaku lagi, kami sarankan Anda segera mengambil tindakan. Identifikasi perubahan kebijakan dan perbarui alur kerja Anda. Jika AWS menyediakan kebijakan penggantian, rencanakan untuk melampirkannya ke semua identitas yang terpengaruh (pengguna, grup, dan peran), lalu lepaskan kebijakan yang tidak digunakan lagi dari identitas tersebut.

Kebijakan usang memiliki karakteristik sebagai berikut:

- Itu dihapus dari panduan ini.
- Izin terus berfungsi untuk semua identitas yang saat ini dilampirkan.
- Di akun tempat kebijakan dilampirkan ke identitas, muncul di daftar Kebijakan di konsol IAM dengan ikon peringatan di sebelahnya.
- Itu tidak dapat dilampirkan pada identitas baru apa pun. Jika Anda melepaskannya dari identitas saat ini, Anda tidak dapat memasangnya kembali.
- Setelah Anda melepaskannya dari semua entitas saat ini, itu tidak lagi terlihat.

AWS kebijakan terkelola

AWS kebijakan terkelola

- AccessAnalyzerServiceRolePolicy
- AdministratorAccess
- AdministratorAccess-Amplify
- AdministratorAccess-AWSElasticBeanstalk
- AlexaForBusinessDeviceSetup
- AlexaForBusinessFullAccess
- AlexaForBusinessGatewayExecution
- AlexaForBusinessLifesizeDelegatedAccessPolicy
- AlexaForBusinessNetworkProfileServicePolicy
- AlexaForBusinessPolyDelegatedAccessPolicy
- AlexaForBusinessReadOnlyAccess
- AmazonAPIGatewayAdministrator
- AmazonAPIGatewayInvokeFullAccess
- AmazonAPIGatewayPushToCloudWatchLogs
- AmazonAppFlowFullAccess
- AmazonAppFlowReadOnlyAccess
- AmazonAppStreamFullAccess
- AmazonAppStreamPCAAccess
- AmazonAppStreamReadOnlyAccess
- AmazonAppStreamServiceAccess
- AmazonAthenaFullAccess
- AmazonAugmentedAIFullAccess
- AmazonAugmentedAIHumanLoopFullAccess
- AmazonAugmentedAIIntegratedAPIAccess
- AmazonBedrockFullAccess
- AmazonBedrockReadOnly

- AmazonBraketFullAccess
- AmazonBraketJobsExecutionPolicy
- AmazonBraketServiceRolePolicy
- AmazonChimeFullAccess
- AmazonChimeReadOnly
- AmazonChimeSDK
- AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy
- AmazonChimeSDKMessagingServiceRolePolicy
- AmazonChimeServiceRolePolicy
- AmazonChimeTranscriptionServiceLinkedRolePolicy
- AmazonChimeUserManagement
- AmazonChimeVoiceConnectorServiceLinkedRolePolicy
- AmazonCloudDirectoryFullAccess
- AmazonCloudDirectoryReadOnlyAccess
- AmazonCloudWatchEvidentlyFullAccess
- AmazonCloudWatchEvidentlyReadOnlyAccess
- AmazonCloudWatchEvidentlyServiceRolePolicy
- AmazonCloudWatchRUMFullAccess
- AmazonCloudWatchRUMReadOnlyAccess
- AmazonCloudWatchRUMServiceRolePolicy
- AmazonCodeCatalystFullAccess
- AmazonCodeCatalystReadOnlyAccess
- AmazonCodeCatalystSupportAccess
- AmazonCodeGuruProfilerAgentAccess
- AmazonCodeGuruProfilerFullAccess
- AmazonCodeGuruProfilerReadOnlyAccess
- AmazonCodeGuruReviewerFullAccess
- AmazonCodeGuruReviewerReadOnlyAccess
- AmazonCodeGuruReviewerServiceRolePolicy

- AmazonCodeGuruSecurityFullAccess
- AmazonCodeGuruSecurityScanAccess
- AmazonCognitoDeveloperAuthenticatedIdentities
- AmazonCognitoIdpEmailServiceRolePolicy
- AmazonCognitoIdpServiceRolePolicy
- AmazonCognitoPowerUser
- AmazonCognitoReadOnly
- AmazonCognitoUnAuthedIdentitiesSessionPolicy
- AmazonCognitoUnauthenticatedIdentities
- AmazonConnect_FullAccess
- AmazonConnectCampaignsServiceLinkedRolePolicy
- AmazonConnectReadOnlyAccess
- AmazonConnectServiceLinkedRolePolicy
- AmazonConnectSynchronizationServiceRolePolicy
- AmazonConnectVoiceIDFullAccess
- AmazonDataZoneDomainExecutionRolePolicy
- AmazonDataZoneEnvironmentRolePermissionsBoundary
- AmazonDataZoneFullAccess
- AmazonDataZoneFullUserAccess
- AmazonDataZoneGlueManageAccessRolePolicy
- AmazonDataZonePortalFullAccessPolicy
- AmazonDataZonePreviewConsoleFullAccess
- AmazonDataZoneProjectDeploymentPermissionsBoundary
- AmazonDataZoneProjectRolePermissionsBoundary
- AmazonDataZoneRedshiftGlueProvisioningPolicy
- AmazonDataZoneRedshiftManageAccessRolePolicy
- AmazonDetectiveFullAccess
- AmazonDetectiveInvestigatorAccess
- AmazonDetectiveMemberAccess

- AmazonDetectiveOrganizationsAccess
- AmazonDetectiveServiceLinkedRolePolicy
- AmazonDevOpsGuruConsoleFullAccess
- AmazonDevOpsGuruFullAccess
- AmazonDevOpsGuruOrganizationsAccess
- AmazonDevOpsGuruReadOnlyAccess
- AmazonDevOpsGuruServiceRolePolicy
- AmazonDMSCloudWatchLogsRole
- AmazonDMSRedshiftS3Role
- AmazonDMSVPCManagementRole
- AmazonDocDB-ElasticServiceRolePolicy
- AmazonDocDBConsoleFullAccess
- AmazonDocDBElasticFullAccess
- AmazonDocDBElasticReadOnlyAccess
- AmazonDocDBFullAccess
- AmazonDocDBReadOnlyAccess
- AmazonDRSVPCManagement
- AmazonDynamoDBFullAccess
- AmazonDynamoDBFullAccesswithDataPipeline
- AmazonDynamoDBReadOnlyAccess
- AmazonEBSCSIDriverPolicy
- AmazonEC2ContainerRegistryFullAccess
- AmazonEC2ContainerRegistryPowerUser
- AmazonEC2ContainerRegistryReadOnly
- AmazonEC2ContainerServiceAutoscaleRole
- AmazonEC2ContainerServiceEventsRole
- AmazonEC2ContainerServiceforEC2Role
- AmazonEC2ContainerServiceRole
- AmazonEC2FullAccess

- AmazonEC2ReadOnlyAccess
- AmazonEC2RoleforAWSCodeDeploy
- AmazonEC2RoleforAWSCodeDeployLimited
- AmazonEC2RoleforDataPipelineRole
- AmazonEC2RoleforSSM
- AmazonEC2RolePolicyForLaunchWizard
- AmazonEC2SpotFleetAutoscaleRole
- AmazonEC2SpotFleetTaggingRole
- AmazonECS_FullAccess
- AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity
- AmazonECSInfrastructureRolePolicyForVolumes
- AmazonECSServiceRolePolicy
- AmazonECSTaskExecutionRolePolicy
- AmazonEFSCSIDriverPolicy
- AmazonEKS_CNI_Policy
- AmazonEKSClusterPolicy
- AmazonEKSConnectorServiceRolePolicy
- AmazonEKSFargatePodExecutionRolePolicy
- AmazonEKSForFargateServiceRolePolicy
- AmazonEKSLocalOutpostClusterPolicy
- AmazonEKSLocalOutpostServiceRolePolicy
- AmazonEKSServicePolicy
- AmazonEKSServiceRolePolicy
- AmazonEKSVPCResourceController
- AmazonEKSWorkerNodePolicy
- AmazonElastiCacheFullAccess
- AmazonElastiCacheReadOnlyAccess
- AmazonElasticContainerRegistryPublicFullAccess
- AmazonElasticContainerRegistryPublicPowerUser

- AmazonElasticContainerRegistryPublicReadOnly
- AmazonElasticFileSystemClientFullAccess
- AmazonElasticFileSystemClientReadOnlyAccess
- AmazonElasticFileSystemClientReadWriteAccess
- AmazonElasticFileSystemFullAccess
- AmazonElasticFileSystemReadOnlyAccess
- AmazonElasticFileSystemServiceRolePolicy
- AmazonElasticFileSystemsUtils
- AmazonElasticMapReduceEditorsRole
- AmazonElasticMapReduceforAutoScalingRole
- AmazonElasticMapReduceforEC2Role
- AmazonElasticMapReduceFullAccess
- AmazonElasticMapReducePlacementGroupPolicy
- AmazonElasticMapReduceReadOnlyAccess
- AmazonElasticMapReduceRole
- AmazonElasticsearchServiceRolePolicy
- AmazonElasticTranscoder_FullAccess
- AmazonElasticTranscoder_JobsSubmitter
- AmazonElasticTranscoder_ReadOnlyAccess
- AmazonElasticTranscoderRole
- AmazonEMRCleanupPolicy
- AmazonEMRContainersServiceRolePolicy
- AmazonEMRFullAccessPolicy_v2
- AmazonEMRReadOnlyAccessPolicy_v2
- AmazonEMRServerlessServiceRolePolicy
- AmazonEMRServicePolicy_v2
- AmazonESCognitoAccess
- AmazonESFullAccess
- AmazonESReadOnlyAccess

- AmazonEventBridgeApiDestinationsServiceRolePolicy
- AmazonEventBridgeFullAccess
- AmazonEventBridgePipesFullAccess
- AmazonEventBridgePipesOperatorAccess
- AmazonEventBridgePipesReadOnlyAccess
- AmazonEventBridgeReadOnlyAccess
- AmazonEventBridgeSchedulerFullAccess
- AmazonEventBridgeSchedulerReadOnlyAccess
- AmazonEventBridgeSchemasFullAccess
- AmazonEventBridgeSchemasReadOnlyAccess
- AmazonEventBridgeSchemasServiceRolePolicy
- AmazonFISServiceRolePolicy
- AmazonForecastFullAccess
- AmazonFraudDetectorFullAccessPolicy
- AmazonFreeRTOSFullAccess
- AmazonFreeRTOSOTAUpdate
- AmazonFSxConsoleFullAccess
- AmazonFSxConsoleReadOnlyAccess
- AmazonFSxFullAccess
- AmazonFSxReadOnlyAccess
- AmazonFSxServiceRolePolicy
- AmazonGlacierFullAccess
- AmazonGlacierReadOnlyAccess
- AmazonGrafanaAthenaAccess
- AmazonGrafanaCloudWatchAccess
- AmazonGrafanaRedshiftAccess
- AmazonGrafanaServiceLinkedRolePolicy
- AmazonGuardDutyFullAccess
- AmazonGuardDutyMalwareProtectionServiceRolePolicy

- AmazonGuardDutyReadOnlyAccess
- AmazonGuardDutyServiceRolePolicy
- AmazonHealthLakeFullAccess
- AmazonHealthLakeReadOnlyAccess
- AmazonHoneycodeFullAccess
- AmazonHoneycodeReadOnlyAccess
- AmazonHoneycodeServiceRolePolicy
- AmazonHoneycodeTeamAssociationFullAccess
- AmazonHoneycodeTeamAssociationReadOnlyAccess
- AmazonHoneycodeWorkbookFullAccess
- AmazonHoneycodeWorkbookReadOnlyAccess
- AmazonInspector2AgentlessServiceRolePolicy
- AmazonInspector2FullAccess
- AmazonInspector2ManagedCisPolicy
- AmazonInspector2ReadOnlyAccess
- AmazonInspector2ServiceRolePolicy
- AmazonInspectorFullAccess
- AmazonInspectorReadOnlyAccess
- AmazonInspectorServiceRolePolicy
- AmazonKendraFullAccess
- AmazonKendraReadOnlyAccess
- AmazonKeyspacesFullAccess
- AmazonKeyspacesReadOnlyAccess
- AmazonKeyspacesReadOnlyAccess_v2
- AmazonKinesisAnalyticsFullAccess
- AmazonKinesisAnalyticsReadOnly
- AmazonKinesisFirehoseFullAccess
- AmazonKinesisFirehoseReadOnlyAccess
- AmazonKinesisFullAccess

- AmazonKinesisReadOnlyAccess
- AmazonKinesisVideoStreamsFullAccess
- AmazonKinesisVideoStreamsReadOnlyAccess
- AmazonLaunchWizard_Fullaccess
- AmazonLaunchWizardFullAccessV2
- AmazonLexChannelsAccess
- AmazonLexFullAccess
- AmazonLexReadOnly
- AmazonLexReplicationPolicy
- AmazonLexRunBotsOnly
- AmazonLexV2BotPolicy
- AmazonLookoutEquipmentFullAccess
- AmazonLookoutEquipmentReadOnlyAccess
- AmazonLookoutMetricsFullAccess
- AmazonLookoutMetricsReadOnlyAccess
- AmazonLookoutVisionConsoleFullAccess
- AmazonLookoutVisionConsoleReadOnlyAccess
- AmazonLookoutVisionFullAccess
- AmazonLookoutVisionReadOnlyAccess
- AmazonMachineLearningBatchPredictionsAccess
- AmazonMachineLearningCreateOnlyAccess
- AmazonMachineLearningFullAccess
- AmazonMachineLearningManageRealTimeEndpointOnlyAccess
- AmazonMachineLearningReadOnlyAccess
- AmazonMachineLearningRealTimePredictionOnlyAccess
- AmazonMachineLearningRoleforRedshiftDataSourceV3
- AmazonMacieFullAccess
- AmazonMacieHandshakeRole
- AmazonMacieReadOnlyAccess

- AmazonMacieServiceRole
- AmazonMacieServiceRolePolicy
- AmazonManagedBlockchainConsoleFullAccess
- AmazonManagedBlockchainFullAccess
- AmazonManagedBlockchainReadOnlyAccess
- AmazonManagedBlockchainServiceRolePolicy
- AmazonMCSFullAccess
- AmazonMCSReadOnlyAccess
- AmazonMechanicalTurkFullAccess
- AmazonMechanicalTurkReadOnly
- AmazonMemoryDBFullAccess
- AmazonMemoryDBReadOnlyAccess
- AmazonMobileAnalyticsFinancialReportAccess
- AmazonMobileAnalyticsFullAccess
- AmazonMobileAnalyticsNon-financialReportAccess
- AmazonMobileAnalyticsWriteOnlyAccess
- AmazonMonitronFullAccess
- AmazonMQApiFullAccess
- AmazonMQApiReadOnlyAccess
- AmazonMQFullAccess
- AmazonMQReadOnlyAccess
- AmazonMQServiceRolePolicy
- AmazonMSKConnectReadOnlyAccess
- AmazonMSKFullAccess
- AmazonMSKReadOnlyAccess
- AmazonMWAAServiceRolePolicy
- AmazonNimbleStudio-LaunchProfileWorker
- AmazonNimbleStudio-StudioAdmin
- AmazonNimbleStudio-StudioUser

- AmazonOmicsFullAccess
- AmazonOmicsReadOnlyAccess
- AmazonOneEnterpriseFullAccess
- AmazonOneEnterpriseInstallerAccess
- AmazonOneEnterpriseReadOnlyAccess
- AmazonOpenSearchDashboardsServiceRolePolicy
- AmazonOpenSearchIngestionFullAccess
- AmazonOpenSearchIngestionReadOnlyAccess
- AmazonOpenSearchIngestionServiceRolePolicy
- AmazonOpenSearchServerlessServiceRolePolicy
- AmazonOpenSearchServiceCognitoAccess
- AmazonOpenSearchServiceFullAccess
- AmazonOpenSearchServiceReadOnlyAccess
- AmazonOpenSearchServiceRolePolicy
- AmazonPersonalizeFullAccess
- AmazonPollyFullAccess
- AmazonPollyReadOnlyAccess
- AmazonPrometheusConsoleFullAccess
- AmazonPrometheusFullAccess
- AmazonPrometheusQueryAccess
- AmazonPrometheusRemoteWriteAccess
- AmazonPrometheusScraperServiceRolePolicy
- AmazonQFullAccess
- AmazonQLDBConsoleFullAccess
- AmazonQLDBFullAccess
- AmazonQLDBReadOnly
- AmazonRDSBetaServiceRolePolicy
- AmazonRDSCustomInstanceProfileRolePolicy
- AmazonRDSCustomPreviewServiceRolePolicy

- AmazonRDSCustomServiceRolePolicy
- AmazonRDSDataFullAccess
- AmazonRDSDirectoryServiceAccess
- AmazonRDSEnhancedMonitoringRole
- AmazonRDSFullAccess
- AmazonRDSPerformanceInsightsFullAccess
- AmazonRDSPerformanceInsightsReadOnly
- AmazonRDSPreviewServiceRolePolicy
- AmazonRDSReadOnlyAccess
- AmazonRDSServiceRolePolicy
- AmazonRedshiftAllCommandsFullAccess
- AmazonRedshiftDataFullAccess
- AmazonRedshiftFullAccess
- AmazonRedshiftQueryEditor
- AmazonRedshiftQueryEditorV2FullAccess
- AmazonRedshiftQueryEditorV2NoSharing
- AmazonRedshiftQueryEditorV2ReadSharing
- AmazonRedshiftQueryEditorV2ReadWriteSharing
- AmazonRedshiftReadOnlyAccess
- AmazonRedshiftServiceLinkedRolePolicy
- AmazonRekognitionCustomLabelsFullAccess
- AmazonRekognitionFullAccess
- AmazonRekognitionReadOnlyAccess
- AmazonRekognitionServiceRole
- AmazonRoute53AutoNamingFullAccess
- AmazonRoute53AutoNamingReadOnlyAccess
- AmazonRoute53AutoNamingRegistrantAccess
- AmazonRoute53DomainsFullAccess
- AmazonRoute53DomainsReadOnlyAccess

- AmazonRoute53FullAccess
- AmazonRoute53ReadOnlyAccess
- AmazonRoute53RecoveryClusterFullAccess
- AmazonRoute53RecoveryClusterReadOnlyAccess
- AmazonRoute53RecoveryControlConfigFullAccess
- AmazonRoute53RecoveryControlConfigReadOnlyAccess
- AmazonRoute53RecoveryReadinessFullAccess
- AmazonRoute53RecoveryReadinessReadOnlyAccess
- AmazonRoute53ResolverFullAccess
- AmazonRoute53ResolverReadOnlyAccess
- AmazonS3FullAccess
- AmazonS3ObjectLambdaExecutionRolePolicy
- AmazonS3OutpostsFullAccess
- AmazonS3OutpostsReadOnlyAccess
- AmazonS3ReadOnlyAccess
- AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy
- AmazonSageMakerCanvasAIServicesAccess
- AmazonSageMakerCanvasBedrockAccess
- AmazonSageMakerCanvasDataPrepFullAccess
- AmazonSageMakerCanvasDirectDeployAccess
- AmazonSageMakerCanvasForecastAccess
- AmazonSageMakerCanvasFullAccess
- AmazonSageMakerClusterInstanceRolePolicy
- AmazonSageMakerCoreServiceRolePolicy
- AmazonSageMakerEdgeDeviceFleetPolicy
- AmazonSageMakerFeatureStoreAccess
- AmazonSageMakerFullAccess
- AmazonSageMakerGeospatialExecutionRole
- AmazonSageMakerGeospatialFullAccess

- AmazonSageMakerGroundTruthExecution
- AmazonSageMakerMechanicalTurkAccess
- AmazonSageMakerModelGovernanceUseAccess
- AmazonSageMakerModelRegistryFullAccess
- AmazonSageMakerNotebooksServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy
- AmazonSageMakerPipelinesIntegrations
- AmazonSageMakerReadOnly
- AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy
- AmazonSecurityLakeAdministrator
- AmazonSecurityLakeMetastoreManager
- AmazonSecurityLakePermissionsBoundary
- AmazonSESFullAccess
- AmazonSESReadOnlyAccess
- AmazonSNSFullAccess
- AmazonSNSReadOnlyAccess
- AmazonSNSRole
- AmazonSQSFullAccess
- AmazonSQSReadOnlyAccess
- AmazonSSMAutomationApproverAccess

- AmazonSSMAutomationRole
- AmazonSSMDirectoryServiceAccess
- AmazonSSMFullAccess
- AmazonSSMMaintenanceWindowRole
- AmazonSSMManagedEC2InstanceDefaultPolicy
- AmazonSSMManagedInstanceCore
- AmazonSSMPatchAssociation
- AmazonSSMReadOnlyAccess
- AmazonSSMServiceRolePolicy
- AmazonSumerianFullAccess
- AmazonTextractFullAccess
- AmazonTextractServiceRole
- AmazonTimestreamConsoleFullAccess
- AmazonTimestreamFullAccess
- AmazonTimestreamInfluxDBFullAccess
- AmazonTimestreamInfluxDBServiceRolePolicy
- AmazonTimestreamReadOnlyAccess
- AmazonTranscribeFullAccess
- AmazonTranscribeReadOnlyAccess
- AmazonVPCCrossAccountNetworkInterfaceOperations
- AmazonVPCFullAccess
- AmazonVPCNetworkAccessAnalyzerFullAccessPolicy
- AmazonVPCReachabilityAnalyzerFullAccessPolicy
- AmazonVPCReachabilityAnalyzerPathComponentReadPolicy
- AmazonVPCReadOnlyAccess
- AmazonWorkDocsFullAccess
- AmazonWorkDocsReadOnlyAccess
- AmazonWorkMailEventsServiceRolePolicy
- AmazonWorkMailFullAccess

- AmazonWorkMailMessageFlowFullAccess
- AmazonWorkMailMessageFlowReadOnlyAccess
- AmazonWorkMailReadOnlyAccess
- AmazonWorkSpacesAdmin
- AmazonWorkSpacesApplicationManagerAdminAccess
- AmazonWorkspacesPCAAccess
- AmazonWorkSpacesSelfServiceAccess
- AmazonWorkSpacesServiceAccess
- AmazonWorkSpacesWebReadOnly
- AmazonWorkSpacesWebServiceRolePolicy
- AmazonZocaloFullAccess
- AmazonZocaloReadOnlyAccess
- AmplifyBackendDeployFullAccess
- APIGatewayServiceRolePolicy
- AppIntegrationsServiceLinkedRolePolicy
- ApplicationAutoScalingForAmazonAppStreamAccess
- ApplicationDiscoveryServiceContinuousExportServiceRolePolicy
- AppRunnerNetworkingServiceRolePolicy
- AppRunnerServiceRolePolicy
- AutoScalingConsoleFullAccess
- AutoScalingConsoleReadOnlyAccess
- AutoScalingFullAccess
- AutoScalingNotificationAccessRole
- AutoScalingReadOnlyAccess
- AutoScalingServiceRolePolicy
- AWS_ConfigRole
- AWSAccountActivityAccess
- AWSAccountManagementFullAccess
- AWSAccountManagementReadOnlyAccess

- AWSAccountUsageReportAccess
- AWSAgentlessDiscoveryService
- AWSAppFabricFullAccess
- AWSAppFabricReadOnlyAccess
- AWSAppFabricServiceRolePolicy
- AWSApplicationAutoscalingAppStreamFleetPolicy
- AWSApplicationAutoscalingCassandraTablePolicy
- AWSApplicationAutoscalingComprehendEndpointPolicy
- AWSApplicationAutoScalingCustomResourcePolicy
- AWSApplicationAutoscalingDynamoDBTablePolicy
- AWSApplicationAutoscalingEC2SpotFleetRequestPolicy
- AWSApplicationAutoscalingECSServicePolicy
- AWSApplicationAutoscalingElastiCacheRGPolicy
- AWSApplicationAutoscalingEMRInstanceGroupPolicy
- AWSApplicationAutoscalingKafkaClusterPolicy
- AWSApplicationAutoscalingLambdaConcurrencyPolicy
- AWSApplicationAutoscalingNeptuneClusterPolicy
- AWSApplicationAutoscalingRDSClusterPolicy
- AWSApplicationAutoscalingSageMakerEndpointPolicy
- AWSApplicationDiscoveryAgentAccess
- AWSApplicationDiscoveryAgentlessCollectorAccess
- AWSApplicationDiscoveryServiceFullAccess
- AWSApplicationMigrationAgentInstallationPolicy
- AWSApplicationMigrationAgentPolicy
- AWSApplicationMigrationAgentPolicy_v2
- AWSApplicationMigrationConversionServerPolicy
- AWSApplicationMigrationEC2Access
- AWSApplicationMigrationFullAccess
- AWSApplicationMigrationMGHAccess

- AWSApplicationMigrationReadOnlyAccess
- AWSApplicationMigrationReplicationServerPolicy
- AWSApplicationMigrationServiceEc2InstancePolicy
- AWSApplicationMigrationServiceRolePolicy
- AWSApplicationMigrationSSMAccess
- AWSApplicationMigrationVCenterClientPolicy
- AWSAppMeshEnvoyAccess
- AWSAppMeshFullAccess
- AWSAppMeshPreviewEnvoyAccess
- AWSAppMeshPreviewServiceRolePolicy
- AWSAppMeshReadOnly
- AWSAppMeshServiceRolePolicy
- AWSAppRunnerFullAccess
- AWSAppRunnerReadOnlyAccess
- AWSAppRunnerServicePolicyForECRAccess
- AWSAppSyncAdministrator
- AWSAppSyncInvokeFullAccess
- AWSAppSyncPushToCloudWatchLogs
- AWSAppSyncSchemaAuthor
- AWSAppSyncServiceRolePolicy
- AWSArtifactAccountSync
- AWSArtifactReportsReadOnlyAccess
- AWSArtifactServiceRolePolicy
- AWSAuditManagerAdministratorAccess
- AWSAuditManagerServiceRolePolicy
- AWSAutoScalingPlansEC2AutoScalingPolicy
- AWSBackupAuditAccess
- AWSBackupDataTransferAccess
- AWSBackupFullAccess

- AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupServiceLinkedRolePolicyForBackup
- AWSBackupServiceLinkedRolePolicyForBackupTest
- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore
- AWSBatchFullAccess
- AWSBatchServiceEventTargetRole
- AWSBatchServiceRole
- AWSBillingConductorFullAccess
- AWSBillingConductorReadOnlyAccess
- AWSBillingReadOnlyAccess
- AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM
- AWSBudgetsActionsWithAWSResourceControlAccess
- AWSBudgetsReadOnlyAccess
- AWSBugBustFullAccess
- AWSBugBustPlayerAccess
- AWSBugBustServiceRolePolicy
- AWSCertificateManagerFullAccess
- AWSCertificateManagerPrivateCAAuditor
- AWSCertificateManagerPrivateCAFullAccess
- AWSCertificateManagerPrivateCAPrivilegedUser
- AWSCertificateManagerPrivateCAReadOnly
- AWSCertificateManagerPrivateCAUser
- AWSCertificateManagerReadOnly
- AWSChatbotServiceLinkedRolePolicy

- AWSCleanRoomsFullAccess
- AWSCleanRoomsFullAccessNoQuerying
- AWSCleanRoomsMLFullAccess
- AWSCleanRoomsMLReadOnlyAccess
- AWSCleanRoomsReadOnlyAccess
- AWSCloud9Administrator
- AWSCloud9EnvironmentMember
- AWSCloud9ServiceRolePolicy
- AWSCloud9SSMInstanceProfile
- AWSCloud9User
- AWSCloudFormationFullAccess
- AWSCloudFormationReadOnlyAccess
- AWSCloudFrontLogger
- AWSCloudHSMFullAccess
- AWSCloudHSMReadOnlyAccess
- AWSCloudHSMRole
- AWSCloudMapDiscoverInstanceAccess
- AWSCloudMapFullAccess
- AWSCloudMapReadOnlyAccess
- AWSCloudMapRegisterInstanceAccess
- AWSCloudShellFullAccess
- AWSCloudTrail_FullAccess
- AWSCloudTrail_ReadOnlyAccess
- AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy
- AWSCodeArtifactAdminAccess
- AWSCodeArtifactReadOnlyAccess
- AWSCodeBuildAdminAccess
- AWSCodeBuildDeveloperAccess
- AWSCodeBuildReadOnlyAccess
- AWSCodeCommitFullAccess

- AWSCodeCommitPowerUser
- AWSCodeCommitReadOnly
- AWSCodeDeployDeployerAccess
- AWSCodeDeployFullAccess
- AWSCodeDeployReadOnlyAccess
- AWSCodeDeployRole
- AWSCodeDeployRoleForCloudFormation
- AWSCodeDeployRoleForECS
- AWSCodeDeployRoleForECSLimited
- AWSCodeDeployRoleForLambda
- AWSCodeDeployRoleForLambdaLimited
- AWSCodePipeline_FullAccess
- AWSCodePipeline_ReadOnlyAccess
- AWSCodePipelineApproverAccess
- AWSCodePipelineCustomActionAccess
- AWSCodeStarFullAccess
- AWSCodeStarNotificationsServiceRolePolicy
- AWSCodeStarServiceRole
- AWSCompromisedKeyQuarantine
- AWSCompromisedKeyQuarantineV2
- AWSConfigMultiAccountSetupPolicy
- AWSConfigRemediationServiceRolePolicy
- AWSConfigRoleForOrganizations
- AWSConfigRulesExecutionRole
- AWSConfigServiceRolePolicy
- AWSConfigUserAccess
- AWSConnector
- AWSControlTowerAccountServiceRolePolicy
- AWSControlTowerServiceRolePolicy
- AWSCostAndUsageReportAutomationPolicy

- AWSDataExchangeFullAccess
- AWSDataExchangeProviderFullAccess
- AWSDataExchangeReadOnly
- AWSDataExchangeSubscriberFullAccess
- AWSDataLifecycleManagerServiceRole
- AWSDataLifecycleManagerServiceRoleForAMIManagement
- AWSDataLifecycleManagerSSMFullAccess
- AWSDataPipeline_FullAccess
- AWSDataPipeline_PowerUser
- AWSDataSyncDiscoveryServiceRolePolicy
- AWSDataSyncFullAccess
- AWSDataSyncReadOnlyAccess
- AWSDeepLensLambdaFunctionAccessPolicy
- AWSDeepLensServiceRolePolicy
- AWSDeepRacerAccountAdminAccess
- AWSDeepRacerCloudFormationAccessPolicy
- AWSDeepRacerDefaultMultiUserAccess
- AWSDeepRacerFullAccess
- AWSDeepRacerRoboMakerAccessPolicy
- AWSDeepRacerServiceRolePolicy
- AWSDenyAll
- AWSDeviceFarmFullAccess
- AWSDeviceFarmServiceRolePolicy
- AWSDeviceFarmTestGridServiceRolePolicy
- AWSDirectConnectFullAccess
- AWSDirectConnectReadOnlyAccess
- AWSDirectConnectServiceRolePolicy
- AWSDirectoryServiceFullAccess
- AWSDirectoryServiceReadOnlyAccess
- AWSDiscoveryContinuousExportFirehosePolicy

- AWSDMSFleetAdvisorServiceRolePolicy
- AWSDMSServerlessServiceRolePolicy
- AWSEC2CapacityReservationFleetRolePolicy
- AWSEC2FleetServiceRolePolicy
- AWSEC2SpotFleetServiceRolePolicy
- AWSEC2SpotServiceRolePolicy
- AWSECRPullThroughCache_ServiceRolePolicy
- AWSElasticBeanstalkCustomPlatformforEC2Role
- AWSElasticBeanstalkEnhancedHealth
- AWSElasticBeanstalkMaintenance
- AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy
- AWSElasticBeanstalkManagedUpdatesServiceRolePolicy
- AWSElasticBeanstalkMulticontainerDocker
- AWSElasticBeanstalkReadOnly
- AWSElasticBeanstalkRoleCore
- AWSElasticBeanstalkRoleCWL
- AWSElasticBeanstalkRoleECS
- AWSElasticBeanstalkRoleRDS
- AWSElasticBeanstalkRoleSNS
- AWSElasticBeanstalkRoleWorkerTier
- AWSElasticBeanstalkService
- AWSElasticBeanstalkServiceRolePolicy
- AWSElasticBeanstalkWebTier
- AWSElasticBeanstalkWorkerTier
- AWSElasticDisasterRecoveryAgentInstallationPolicy
- AWSElasticDisasterRecoveryAgentPolicy
- AWSElasticDisasterRecoveryConsoleFullAccess
- AWSElasticDisasterRecoveryConsoleFullAccess_v2
- AWSElasticDisasterRecoveryConversionServerPolicy
- AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

- AWSElasticDisasterRecoveryEc2InstancePolicy
- AWSElasticDisasterRecoveryFailbackInstallationPolicy
- AWSElasticDisasterRecoveryFailbackPolicy
- AWSElasticDisasterRecoveryLaunchActionsPolicy
- AWSElasticDisasterRecoveryNetworkReplicationPolicy
- AWSElasticDisasterRecoveryReadOnlyAccess
- AWSElasticDisasterRecoveryRecoveryInstancePolicy
- AWSElasticDisasterRecoveryReplicationServerPolicy
- AWSElasticDisasterRecoveryServiceRolePolicy
- AWSElasticDisasterRecoveryStagingAccountPolicy
- AWSElasticDisasterRecoveryStagingAccountPolicy_v2
- AWSElasticLoadBalancingClassicServiceRolePolicy
- AWSElasticLoadBalancingServiceRolePolicy
- AWSElementalMediaConvertFullAccess
- AWSElementalMediaConvertReadOnly
- AWSElementalMediaLiveFullAccess
- AWSElementalMediaLiveReadOnly
- AWSElementalMediaPackageFullAccess
- AWSElementalMediaPackageReadOnly
- AWSElementalMediaPackageV2FullAccess
- AWSElementalMediaPackageV2ReadOnly
- AWSElementalMediaStoreFullAccess
- AWSElementalMediaStoreReadOnly
- AWSElementalMediaTailorFullAccess
- AWSElementalMediaTailorReadOnly
- AWSEnhancedClassicNetworkingMangementPolicy
- AWSEntityResolutionConsoleFullAccess
- AWSEntityResolutionConsoleReadOnlyAccess
- AWSFaultInjectionSimulatorEC2Access
- AWSFaultInjectionSimulatorECSAccess

- AWSFaultInjectionSimulatorEKSAccess
- AWSFaultInjectionSimulatorNetworkAccess
- AWSFaultInjectionSimulatorRDSAccess
- AWSFaultInjectionSimulatorSSMAccess
- AWSFinSpaceServiceRolePolicy
- AWSFMAdminFullAccess
- AWSFMAdminReadOnlyAccess
- AWSFMMemberReadOnlyAccess
- AWSForWordPressPluginPolicy
- AWSGitSyncServiceRolePolicy
- AWSGlobalAcceleratorSLRPolicy
- AWSGlueConsoleFullAccess
- AWSGlueConsoleSageMakerNotebookFullAccess
- AwsGlueDataBrewFullAccessPolicy
- AWSGlueDataBrewServiceRole
- AWSGlueSchemaRegistryFullAccess
- AWSGlueSchemaRegistryReadonlyAccess
- AWSGlueServiceNotebookRole
- AWSGlueServiceRole
- AwsGlueSessionUserRestrictedNotebookPolicy
- AwsGlueSessionUserRestrictedNotebookServiceRole
- AwsGlueSessionUserRestrictedPolicy
- AwsGlueSessionUserRestrictedServiceRole
- AWSGrafanaAccountAdministrator
- AWSGrafanaConsoleReadOnlyAccess
- AWSGrafanaWorkspacePermissionManagement
- AWSGrafanaWorkspacePermissionManagementV2
- AWSGreengrassFullAccess
- AWSGreengrassReadOnlyAccess
- AWSGreengrassResourceAccessRolePolicy

- AWSGroundStationAgentInstancePolicy
- AWSHealth_EventProcessorServiceRolePolicy
- AWSHealthFullAccess
- AWSHealthImagingFullAccess
- AWSHealthImagingReadOnlyAccess
- AWSIAMIdentityCenterAllowListForIdentityContext
- AWSIdentitySyncFullAccess
- AWSIdentitySyncReadOnlyAccess
- AWSImageBuilderFullAccess
- AWSImageBuilderReadOnlyAccess
- AWSImportExportFullAccess
- AWSImportExportReadOnlyAccess
- AWSIncidentManagerIncidentAccessServiceRolePolicy
- AWSIncidentManagerResolverAccess
- AWSIncidentManagerServiceRolePolicy
- AWSIoT1ClickFullAccess
- AWSIoT1ClickReadOnlyAccess
- AWSIoTAnalyticsFullAccess
- AWSIoTAnalyticsReadOnlyAccess
- AWSIoTConfigAccess
- AWSIoTConfigReadOnlyAccess
- AWSIoTDataAccess
- AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction
- AWSIoTDeviceDefenderAudit
- AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction
- AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction
- AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction
- AWSIoTDeviceDefenderUpdateCACertMitigationAction
- AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction
- AWSIoTDeviceTesterForFreeRTOSFullAccess

- AWSIoTDeviceTesterForGreengrassFullAccess
- AWSIoTEventsFullAccess
- AWSIoTEventsReadOnlyAccess
- AWSIoTFleetHubFederationAccess
- AWSIoTFleetwiseServiceRolePolicy
- AWSIoTFullAccess
- AWSIoTLogging
- AWSIoTOTAUpdate
- AWSIotRoboRunnerFullAccess
- AWSIotRoboRunnerReadOnly
- AWSIotRoboRunnerServiceRolePolicy
- AWSIoTRuleActions
- AWSIoTSiteWiseConsoleFullAccess
- AWSIoTSiteWiseFullAccess
- AWSIoTSiteWiseMonitorPortalAccess
- AWSIoTSiteWiseMonitorServiceRolePolicy
- AWSIoTSiteWiseReadOnlyAccess
- AWSIoTThingsRegistration
- AWSIoTTwinMakerServiceRolePolicy
- AWSIoTWirelessDataAccess
- AWSIoTWirelessFullAccess
- AWSIoTWirelessFullPublishAccess
- AWSIoTWirelessGatewayCertManager
- AWSIoTWirelessLogging
- AWSIoTWirelessReadOnlyAccess
- AWSIPAMServiceRolePolicy
- AWSIQContractServiceRolePolicy
- AWSIQFullAccess
- AWSIQPermissionServiceRolePolicy
- AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

- AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy
- AWSKeyManagementServicePowerUser
- AWSLakeFormationCrossAccountManager
- AWSLakeFormationDataAdmin
- AWSLambda_FullAccess
- AWSLambda_ReadOnlyAccess
- AWSLambdaBasicExecutionRole
- AWSLambdaDynamoDBExecutionRole
- AWSLambdaENIManagementAccess
- AWSLambdaExecute
- AWSLambdaFullAccess
- AWSLambdaInvocation-DynamoDB
- AWSLambdaKinesisExecutionRole
- AWSLambdaMSKExecutionRole
- AWSLambdaReplicator
- AWSLambdaRole
- AWSLambdaSQSQueueExecutionRole
- AWSLambdaVPCAccessExecutionRole
- AWSLicenseManagerConsumptionPolicy
- AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy
- AWSLicenseManagerMasterAccountRolePolicy
- AWSLicenseManagerMemberAccountRolePolicy
- AWSLicenseManagerServiceRolePolicy
- AWSLicenseManagerUserSubscriptionsServiceRolePolicy
- AWSM2ServicePolicy
- AWSManagedServices_ContactsServiceRolePolicy
- AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy
- AWSManagedServices_EventsServiceRolePolicy
- AWSManagedServicesDeploymentToolkitPolicy
- AWSMarketplaceAmiIngestion

- AWSMarketplaceDeploymentServiceRolePolicy
- AWSMarketplaceFullAccess
- AWSMarketplaceGetEntitlements
- AWSMarketplaceImageBuildFullAccess
- AWSMarketplaceLicenseManagementServiceRolePolicy
- AWSMarketplaceManageSubscriptions
- AWSMarketplaceMeteringFullAccess
- AWSMarketplaceMeteringRegisterUsage
- AWSMarketplaceProcurementSystemAdminFullAccess
- AWSMarketplacePurchaseOrdersServiceRolePolicy
- AWSMarketplaceRead-only
- AWSMarketplaceResaleAuthorizationServiceRolePolicy
- AWSMarketplaceSellerFullAccess
- AWSMarketplaceSellerProductsFullAccess
- AWSMarketplaceSellerProductsReadOnly
- AWSMediaConnectServicePolicy
- AWSMediaTailorServiceRolePolicy
- AWSMigrationHubDiscoveryAccess
- AWSMigrationHubDMSAccess
- AWSMigrationHubFullAccess
- AWSMigrationHubOrchestratorConsoleFullAccess
- AWSMigrationHubOrchestratorInstanceRolePolicy
- AWSMigrationHubOrchestratorPlugin
- AWSMigrationHubOrchestratorServiceRolePolicy
- AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess
- AWSMigrationHubRefactorSpaces-SSMAutomationPolicy
- AWSMigrationHubRefactorSpacesFullAccess
- AWSMigrationHubRefactorSpacesServiceRolePolicy
- AWSMigrationHubSMSAccess
- AWSMigrationHubStrategyCollector

- AWSMigrationHubStrategyConsoleFullAccess
- AWSMigrationHubStrategyServiceRolePolicy
- AWSMobileHub_FullAccess
- AWSMobileHub_ReadOnly
- AWSMSKReplicatorExecutionRole
- AWSNetworkFirewallServiceRolePolicy
- AWSNetworkManagerCloudWANServiceRolePolicy
- AWSNetworkManagerFullAccess
- AWSNetworkManagerReadOnlyAccess
- AWSNetworkManagerServiceRolePolicy
- AWSOpsWorks_FullAccess
- AWSOpsWorksCloudWatchLogs
- AWSOpsWorksCMInstanceProfileRole
- AWSOpsWorksCMServiceRole
- AWSOpsWorksInstanceRegistration
- AWSOpsWorksRegisterCLI_EC2
- AWSOpsWorksRegisterCLI_OnPremises
- AWSOrganizationsFullAccess
- AWSOrganizationsReadOnlyAccess
- AWSOrganizationsServiceTrustPolicy
- AWSOutpostsAuthorizeServerPolicy
- AWSOutpostsServiceRolePolicy
- AWSPanoramaApplianceRolePolicy
- AWSPanoramaApplianceServiceRolePolicy
- AWSPanoramaFullAccess
- AWSPanoramaGreengrassGroupRolePolicy
- AWSPanoramaSageMakerRolePolicy
- AWSPanoramaServiceLinkedRolePolicy
- AWSPanoramaServiceRolePolicy
- AWSPriceListServiceFullAccess

- AWSPrivateCAAuditor
- AWSPrivateCAFullAccess
- AWSPrivateCAPrivilegedUser
- AWSPrivateCAReadOnly
- AWSPrivateCAUser
- AWSPrivateMarketplaceAdminFullAccess
- AWSPrivateMarketplaceRequests
- AWSPrivateNetworksServiceRolePolicy
- AWSProtonCodeBuildProvisioningBasicAccess
- AWSProtonCodeBuildProvisioningServiceRolePolicy
- AWSProtonDeveloperAccess
- AWSProtonFullAccess
- AWSProtonReadOnlyAccess
- AWSProtonServiceGitSyncServiceRolePolicy
- AWSProtonSyncServiceRolePolicy
- AWSPurchaseOrdersServiceRolePolicy
- AWSQuicksightAthenaAccess
- AWSQuickSightDescribeRDS
- AWSQuickSightDescribeRedshift
- AWSQuickSightElasticsearchPolicy
- AWSQuickSightIoTAnalyticsAccess
- AWSQuickSightListIAM
- AWSQuicksightOpenSearchPolicy
- AWSQuickSightSageMakerPolicy
- AWSQuickSightTimestreamPolicy
- AWSReachabilityAnalyzerServiceRolePolicy
- AWSRefactoringToolkitFullAccess
- AWSRefactoringToolkitSidecarPolicy
- AWSrePostPrivateCloudWatchAccess
- AWSRepostSpaceSupportOperationsPolicy

- AWSResilienceHubAsssessmentExecutionPolicy
- AWSResourceAccessManagerFullAccess
- AWSResourceAccessManagerReadOnlyAccess
- AWSResourceAccessManagerResourceShareParticipantAccess
- AWSResourceAccessManagerServiceRolePolicy
- AWSResourceExplorerFullAccess
- AWSResourceExplorerOrganizationsAccess
- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerServiceRolePolicy
- AWSResourceGroupsReadOnlyAccess
- AWSRoboMaker_FullAccess
- AWSRoboMakerReadOnlyAccess
- AWSRoboMakerServicePolicy
- AWSRoboMakerServiceRolePolicy
- AWSRolesAnywhereServicePolicy
- AWSS3OnOutpostsServiceRolePolicy
- AWSSavingsPlansFullAccess
- AWSSavingsPlansReadOnlyAccess
- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess
- AWSSecurityHubReadOnlyAccess
- AWSSecurityHubServiceRolePolicy
- AWSServiceCatalogAdminFullAccess
- AWSServiceCatalogAdminReadOnlyAccess
- AWSServiceCatalogAppRegistryFullAccess
- AWSServiceCatalogAppRegistryReadOnlyAccess
- AWSServiceCatalogAppRegistryServiceRolePolicy
- AWSServiceCatalogEndUserFullAccess
- AWSServiceCatalogEndUserReadOnlyAccess
- AWSServiceCatalogOrgsDataSyncServiceRolePolicy

- AWSServiceCatalogSyncServiceRolePolicy
- AWSServiceRoleForAmazonEKSNodegroup
- AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy
- AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy
- AWSServiceRoleForCodeGuru-Profiler
- AWSServiceRoleForCodeWhispererPolicy
- AWSServiceRoleForEC2ScheduledInstances
- AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy
- AWSServiceRoleForImageBuilder
- AWSServiceRoleForIoTSiteWise
- AWSServiceRoleForLogDeliveryPolicy
- AWSServiceRoleForMonitronPolicy
- AWSServiceRoleForNeptuneGraphPolicy
- AWSServiceRoleForPrivateMarketplaceAdminPolicy
- AWSServiceRoleForSMS
- AWSServiceRolePolicyForBackupReports
- AWSServiceRolePolicyForBackupRestoreTesting
- AWSShieldDRTAccessPolicy
- AWSShieldServiceRolePolicy
- AWSSSMForSAPServiceLinkedRolePolicy
- AWSSSMOpsInsightsServiceRolePolicy
- AWSSSODirectoryAdministrator
- AWSSSODirectoryReadOnly
- AWSSSOMasterAccountAdministrator
- AWSSSOMemberAccountAdministrator
- AWSSSOReadOnly
- AWSSSOServiceRolePolicy
- AWSStepFunctionsConsoleFullAccess
- AWSStepFunctionsFullAccess
- AWSStepFunctionsReadOnlyAccess

- AWSStorageGatewayFullAccess
- AWSStorageGatewayReadOnlyAccess
- AWSStorageGatewayServiceRolePolicy
- AWSSupplyChainFederationAdminAccess
- AWSSupportAccess
- AWSSupportAppFullAccess
- AWSSupportAppReadOnlyAccess
- AWSSupportPlansFullAccess
- AWSSupportPlansReadOnlyAccess
- AWSSupportServiceRolePolicy
- AWSSystemsManagerAccountDiscoveryServicePolicy
- AWSSystemsManagerChangeManagementServicePolicy
- AWSSystemsManagerForSAPFullAccess
- AWSSystemsManagerForSAPReadOnlyAccess
- AWSSystemsManagerOpsDataSyncServiceRolePolicy
- AWSThinkboxAssetServerPolicy
- AWSThinkboxAWSPortalAdminPolicy
- AWSThinkboxAWSPortalGatewayPolicy
- AWSThinkboxAWSPortalWorkerPolicy
- AWSThinkboxDeadlineResourceTrackerAccessPolicy
- AWSThinkboxDeadlineResourceTrackerAdminPolicy
- AWSThinkboxDeadlineSpotEventPluginAdminPolicy
- AWSThinkboxDeadlineSpotEventPluginWorkerPolicy
- AWSTransferConsoleFullAccess
- AWSTransferFullAccess
- AWSTransferLoggingAccess
- AWSTransferReadOnlyAccess
- AWSTrustedAdvisorPriorityFullAccess
- AWSTrustedAdvisorPriorityReadOnlyAccess
- AWSTrustedAdvisorReportingServiceRolePolicy

- AWSTrustedAdvisorServiceRolePolicy
- AWSUserNotificationsServiceLinkedRolePolicy
- AWSVendorInsightsAssessorFullAccess
- AWSVendorInsightsAssessorReadOnly
- AWSVendorInsightsVendorFullAccess
- AWSVendorInsightsVendorReadOnly
- AWSVpcLatticeServiceRolePolicy
- AWSVPCS2SVpnServiceRolePolicy
- AWSVPCTransitGatewayServiceRolePolicy
- AWSVPCVerifiedAccessServiceRolePolicy
- AWSWAFConsoleFullAccess
- AWSWAFConsoleReadOnlyAccess
- AWSWAFFullAccess
- AWSWAFReadOnlyAccess
- AWSWellArchitectedDiscoveryServiceRolePolicy
- AWSWellArchitectedOrganizationsServiceRolePolicy
- AWSWickrFullAccess
- AWSXrayCrossAccountSharingConfiguration
- AWSXRayDaemonWriteAccess
- AWSXrayFullAccess
- AWSXrayReadOnlyAccess
- AWSXrayWriteOnlyAccess
- AWSZonalAutoshiftPracticeRunSLRPolicy
- BatchServiceRolePolicy
- Billing
- CertificateManagerServiceRolePolicy
- ClientVPNServiceConnectionsRolePolicy
- ClientVPNServiceRolePolicy
- CloudFormationStackSetsOrgAdminServiceRolePolicy
- CloudFormationStackSetsOrgMemberServiceRolePolicy

- CloudFrontFullAccess
- CloudFrontReadOnlyAccess
- CloudHSMServiceRolePolicy
- CloudSearchFullAccess
- CloudSearchReadOnlyAccess
- CloudTrailServiceRolePolicy
- CloudWatch-CrossAccountAccess
- CloudWatchActionsEC2Access
- CloudWatchAgentAdminPolicy
- CloudWatchAgentServerPolicy
- CloudWatchApplicationInsightsFullAccess
- CloudWatchApplicationInsightsReadOnlyAccess
- CloudwatchApplicationInsightsServiceLinkedRolePolicy
- CloudWatchApplicationSignalsServiceRolePolicy
- CloudWatchAutomaticDashboardsAccess
- CloudWatchCrossAccountSharingConfiguration
- CloudWatchEventsBuiltInTargetExecutionAccess
- CloudWatchEventsFullAccess
- CloudWatchEventsInvocationAccess
- CloudWatchEventsReadOnlyAccess
- CloudWatchEventsServiceRolePolicy
- CloudWatchFullAccess
- CloudWatchFullAccessV2
- CloudWatchInternetMonitorServiceRolePolicy
- CloudWatchLambdaInsightsExecutionRolePolicy
- CloudWatchLogsCrossAccountSharingConfiguration
- CloudWatchLogsFullAccess
- CloudWatchLogsReadOnlyAccess
- CloudWatchNetworkMonitorServiceRolePolicy
- CloudWatchReadOnlyAccess

- CloudWatchSyntheticsFullAccess
- CloudWatchSyntheticsReadOnlyAccess
- ComprehendDataAccessRolePolicy
- ComprehendFullAccess
- ComprehendMedicalFullAccess
- ComprehendReadOnly
- ComputeOptimizerReadOnlyAccess
- ComputeOptimizerServiceRolePolicy
- ConfigConformsServiceRolePolicy
- CostOptimizationHubAdminAccess
- CostOptimizationHubReadOnlyAccess
- CostOptimizationHubServiceRolePolicy
- CustomerProfilesServiceLinkedRolePolicy
- DatabaseAdministrator
- DataScientist
- DAXServiceRolePolicy
- DynamoDBCloudWatchContributorInsightsServiceRolePolicy
- DynamoDBKinesisReplicationServiceRolePolicy
- DynamoDBReplicationServiceRolePolicy
- EC2FastLaunchServiceRolePolicy
- EC2FleetTimeShiftableServiceRolePolicy
- Ec2ImageBuilderCrossAccountDistributionAccess
- EC2ImageBuilderLifecycleExecutionPolicy
- EC2InstanceConnect
- Ec2InstanceConnectEndpoint
- EC2InstanceProfileForImageBuilder
- EC2InstanceProfileForImageBuilderECRContainerBuilds
- ECRReplicationServiceRolePolicy
- ElastiCacheServiceRolePolicy
- ElasticLoadBalancingFullAccess

- ElasticLoadBalancingReadOnly
- ElementalActivationsDownloadSoftwareAccess
- ElementalActivationsFullAccess
- ElementalActivationsGenerateLicenses
- ElementalActivationsReadOnlyAccess
- ElementalAppliancesSoftwareFullAccess
- ElementalAppliancesSoftwareReadOnlyAccess
- ElementalSupportCenterFullAccess
- EMRDescribeClusterPolicyForEMRWAL
- FMSServiceRolePolicy
- FSxDeleteServiceLinkedRoleAccess
- GameLiftGameServerGroupPolicy
- GlobalAcceleratorFullAccess
- GlobalAcceleratorReadOnlyAccess
- GreengrassOTAUpdateArtifactAccess
- GroundTruthSyntheticConsoleFullAccess
- GroundTruthSyntheticConsoleReadOnlyAccess
- Health_OrganizationsServiceRolePolicy
- IAMAccessAdvisorReadOnly
- IAMAccessAnalyzerFullAccess
- IAMAccessAnalyzerReadOnlyAccess
- IAMFullAccess
- IAMReadOnlyAccess
- IAMSelfManageServiceSpecificCredentials
- IAMUserChangePassword
- IAMUserSSHKeys
- IVSFullAccess
- IVSReadOnlyAccess
- IVSRecordToS3
- KafkaConnectServiceRolePolicy

- KafkaServiceRolePolicy
- KeyspacesReplicationServiceRolePolicy
- LakeFormationDataAccessServiceRolePolicy
- LexBotPolicy
- LexChannelPolicy
- LightsailExportAccess
- MediaConnectGatewayInstanceRolePolicy
- MediaPackageServiceRolePolicy
- MemoryDBServiceRolePolicy
- MigrationHubDMSAccessServiceRolePolicy
- MigrationHubServiceRolePolicy
- MigrationHubSMSAccessServiceRolePolicy
- MonitronServiceRolePolicy
- NeptuneConsoleFullAccess
- NeptuneFullAccess
- NeptuneGraphReadOnlyAccess
- NeptuneReadOnlyAccess
- NetworkAdministrator
- OAMFullAccess
- OAMReadOnlyAccess
- PartnerCentralAccountManagementUserRoleAssociation
- PowerUserAccess
- QuickSightAccessForS3StorageManagementAnalyticsReadOnly
- RDSCloudHsmAuthorizationRole
- ReadOnlyAccess
- ResourceGroupsandTagEditorFullAccess
- ResourceGroupsandTagEditorReadOnlyAccess
- ResourceGroupsServiceRolePolicy
- ROSAAmazonEBSCSIDriverOperatorPolicy
- ROSACloudNetworkConfigOperatorPolicy

- ROSAControlPlaneOperatorPolicy
- ROSAImageRegistryOperatorPolicy
- ROSAIngressOperatorPolicy
- ROSAInstallerPolicy
- ROSAKMSProviderPolicy
- ROSAKubeControllerPolicy
- ROSAManageSubscription
- ROSANodePoolManagementPolicy
- ROSASRESupportPolicy
- ROSAWorkerInstancePolicy
- Route53RecoveryReadinessServiceRolePolicy
- Route53ResolverServiceRolePolicy
- S3StorageLensServiceRolePolicy
- SecretsManagerReadWrite
- SecurityAudit
- SecurityLakeServiceLinkedRole
- ServerMigration_ServiceRole
- ServerMigrationConnector
- ServerMigrationServiceConsoleFullAccess
- ServerMigrationServiceLaunchRole
- ServerMigrationServiceRoleForInstanceValidation
- ServiceQuotasFullAccess
- ServiceQuotasReadOnlyAccess
- ServiceQuotasServiceRolePolicy
- SimpleWorkflowFullAccess
- SupportUser
- SystemAdministrator
- TranslateFullAccess
- TranslateReadOnly
- ViewOnlyAccess

- VMImportExportRoleForAWSConnector
- VPCLatticeFullAccess
- VPCLatticeReadOnlyAccess
- VPCLatticeServicesInvokeAccess
- WAFLoggingServiceRolePolicy
- WAFRegionalLoggingServiceRolePolicy
- WAFV2LoggingServiceRolePolicy
- WellArchitectedConsoleFullAccess
- WellArchitectedConsoleReadOnlyAccess
- WorkLinkServiceRolePolicy

AccessAnalyzerServiceRolePolicy

`AccessAnalyzerServiceRolePolicy`adalah kebijakan AWS terkelola yang: Izinkan Access Analyzer menganalisis metadata sumber daya

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 02 Desember 2019, 17:13 UTC
- Waktu telah diedit: 22 Januari 2024, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessAnalyzerServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ecr:DescribeRepositories",
        "ecr:GetRepositoryPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "iam:GetRole",
        "iam:ListEntitiesForPolicy",
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:GetUser",
        "iam:GetGroup",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetails",
        "iam:ListAccessKeys",
        "iam:GetLoginProfile",
        "iam:GetAccessKeyLastUsed",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
```

```
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListVersionsByFunction",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "s3:DescribeMultiRegionAccessPointOperation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints",
        "s3express:GetBucketPolicy",
        "s3express:ListAllMyDirectoryBuckets",
        "sns:GetTopicAttributes",
        "sns:ListTopics",
        "secretsmanager:DescribeSecret",
```

```
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AdministratorAccess

`AdministratorAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke AWS layanan dan sumber daya.

Menggunakan kebijakan ini

Anda dapat melampirkan `AdministratorAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu telah diedit: 06 Februari 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AdministratorAccess-Amplify

`AdministratorAccess-Amplify`adalah kebijakan AWS terkelola yang: Memberikan izin administratif akun sambil secara eksplisit mengizinkan akses langsung ke sumber daya yang dibutuhkan oleh aplikasi Amplify.

Menggunakan kebijakan ini

Anda dapat melampirkan `AdministratorAccess-Amplify` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2020, 19:03 UTC
- Waktu yang telah diedit: 31 Mei 2023, 17.08 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-Amplify`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CLICloudformationPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackSet",
        "cloudformation:UpdateStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/amplify-*"
      ]
    },
    {
      "Sid" : "CLIManageviaCFNPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoleTags",
```

```
        "iam:TagRole",
        "iam:AttachRolePolicy",
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePolicy",
        "iam:UntagRole",
        "iam:UpdateRole",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetRolePolicy",
        "iam:PassRole",
        "iam:ListPolicyVersions",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion",
        "iam:CreateRole",
        "iam:ListRolePolicies",
        "iam:PutRolePermissionsBoundary",
        "iam:DeleteRolePermissionsBoundary",
        "appsync:CreateApiKey",
        "appsync:CreateDataSource",
        "appsync:CreateFunction",
        "appsync:CreateResolver",
        "appsync:CreateType",
        "appsync:DeleteApiKey",
        "appsync:DeleteDataSource",
        "appsync:DeleteFunction",
        "appsync:DeleteResolver",
        "appsync:DeleteType",
        "appsync:GetDataSource",
        "appsync:GetFunction",
        "appsync:GetIntrospectionSchema",
        "appsync:GetResolver",
        "appsync:GetSchemaCreationStatus",
        "appsync:GetType",
        "appsync:GraphQL",
        "appsync:ListApiKeys",
        "appsync:ListDataSources",
        "appsync:ListFunctions",
        "appsync:ListGraphqlApis",
        "appsync:ListResolvers",
        "appsync:ListResolversByFunction",
```

```
        "appsync:ListTypes",
        "appsync:StartSchemaCreation",
        "appsync:UntagResource",
        "appsync:UpdateApiKey",
        "appsync:UpdateDataSource",
        "appsync:UpdateFunction",
        "appsync:UpdateResolver",
        "appsync:UpdateType",
        "appsync:TagResource",
        "appsync:CreateGraphqlApi",
        "appsync:DeleteGraphqlApi",
        "appsync:GetGraphqlApi",
        "appsync:ListTagsForResource",
        "appsync:UpdateGraphqlApi",
        "apigateway:DELETE",
        "apigateway:GET",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "cognito-idp:CreateUserPool",
        "cognito-identity:CreateIdentityPool",
        "cognito-identity:DeleteIdentityPool",
        "cognito-identity:DescribeIdentity",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:SetIdentityPoolRoles",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:UpdateIdentityPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:UpdateUserPoolClient",
        "cognito-idp:CreateGroup",
        "cognito-idp:DeleteGroup",
        "cognito-identity:TagResource",
        "cognito-idp:TagResource",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:SetUserPoolMfaConfig",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
```

```
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeAsync",
        "lambda:InvokeFunction",
        "lambda:RemovePermission",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:AddLayerVersionPermission",
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping",
        "lambda:DeleteLayerVersion",
        "lambda:GetEventSourceMapping",
        "lambda:GetLayerVersion",
        "lambda:ListEventSourceMappings",
        "lambda:ListLayerVersions",
        "lambda:PublishLayerVersion",
        "lambda:RemoveLayerVersionPermission",
        "lambda:UpdateEventSourceMapping",
        "dynamodb:CreateTable",
        "dynamodb:DeleteItem",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListStreams",
        "dynamodb:PutItem",
        "dynamodb:TagResource",
        "dynamodb:ListTagsOfResource",
        "dynamodb:UntagResource",
        "dynamodb:UpdateContinuousBackups",
        "dynamodb:UpdateItem",
        "dynamodb:UpdateTable",
        "dynamodb:UpdateTimeToLive",
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
        "s3:PutBucketWebsite",
        "s3:PutObjectAcl",
```

```
        "cloudfront:CreateCloudFrontOriginAccessIdentity",
        "cloudfront:CreateDistribution",
        "cloudfront:DeleteCloudFrontOriginAccessIdentity",
        "cloudfront:DeleteDistribution",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetCloudFrontOriginAccessIdentityConfig",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:TagResource",
        "cloudfront:UntagResource",
        "cloudfront:UpdateCloudFrontOriginAccessIdentity",
        "cloudfront:UpdateDistribution",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "mobiletargeting:GetApp",
        "kinesis:AddTagsToStream",
        "kinesis:CreateStream",
        "kinesis:DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListTagsForStream",
        "kinesis:PutRecords",
        "es:AddTags",
        "es:CreateElasticsearchDomain",
        "es:DeleteElasticsearchDomain",
        "es:DescribeElasticsearchDomain",
        "es:UpdateElasticsearchDomainConfig",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "CLISDKCalls",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetIntrospectionSchema",
        "appsync:GraphQL",
        "appsync:UpdateApiKey",
        "appsync:ListApiKeys",
        "amplify:*",
        "amplifybackend:*",
        "amplifyuibuilder:*",
        "sts:AssumeRole",
        "mobiletargeting:*",
        "cognito-idp:AdminAddUserToGroup",
        "cognito-idp:AdminCreateUser",
        "cognito-idp:CreateGroup",
        "cognito-idp:DeleteGroup",
        "cognito-idp:DeleteUser",
        "cognito-idp:ListUsers",
        "cognito-idp:AdminGetUser",
        "cognito-idp:ListUsersInGroup",
        "cognito-idp:AdminDisableUser",
        "cognito-idp:AdminRemoveUserFromGroup",
        "cognito-idp:AdminResetUserPassword",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:ListGroups",
        "cognito-idp:AdminListUserAuthEvents",
        "cognito-idp:AdminDeleteUser",
        "cognito-idp:AdminConfirmSignUp",
        "cognito-idp:AdminEnableUser",
        "cognito-idp:AdminUpdateUserAttributes",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:CreateUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:AdminSetUserPassword",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:SetIdentityPoolRoles",
```

```
        "cognito-identity:CreateIdentityPool",
        "cognito-identity:DeleteIdentityPool",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:DescribeIdentityPool",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "lambda:GetFunction",
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "lambda:DeleteFunction",
        "lambda:DeleteLayerVersion",
        "lambda:InvokeFunction",
        "lambda:ListLayerVersions",
        "iam:PutRolePolicy",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy",
        "iam:ListPolicyVersions",
        "iam:ListAttachedRolePolicies",
        "iam:CreateRole",
        "iam:PassRole",
        "iam:ListRolePolicies",
        "iam:DeleteRolePolicy",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion",
        "iam:DeleteRole",
        "iam:DetachRolePolicy",
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks",
        "sns:CreateSMSSandboxPhoneNumber",
        "sns:GetSMSSandboxAccountStatus",
        "sns:VerifySMSSandboxPhoneNumber",
        "sns:DeleteSMSSandboxPhoneNumber",
        "sns:ListSMSSandboxPhoneNumbers",
        "sns:ListOriginationNumbers",
        "rekognition:DescribeCollection",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "lex:GetBot",
        "lex:GetBuiltinIntent",
        "lex:GetBuiltinIntents",
        "lex:GetBuiltinSlotTypes",
        "cloudformation:GetTemplateSummary",
        "codecommit:GitPull",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
```

```
        "cloudfront:GetCloudFrontOriginAccessIdentityConfig",
        "polly:DescribeVoices"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifySSMCalls",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:GetParametersByPath",
        "ssm:GetParameters",
        "ssm:GetParameter",
        "ssm:DeleteParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*"
    },
    {
      "Sid" : "GeoPowerUser",
      "Effect" : "Allow",
      "Action" : [
        "geo:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifyEcrSDKCalls",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifyStorageSDKCalls",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteBucketWebsite",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
```

```
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutBucketWebsite",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifySSRCalls",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:CreateCloudFrontOriginAccessIdentity",
        "cloudfront:CreateDistribution",
        "cloudfront:CreateInvalidation",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByLambdaFunction",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListFieldLevelEncryptionConfigs",
        "cloudfront:ListFieldLevelEncryptionProfiles",
        "cloudfront:ListInvalidations",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListStreamingDistributions",
        "cloudfront:UpdateDistribution",
        "cloudfront:TagResource",
        "cloudfront:UntagResource",
        "cloudfront:ListTagsForResource",
        "cloudfront:DeleteDistribution",
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:CreateServiceLinkedRole",
```

```
        "iam:GetRole",
        "iam:PutRolePolicy",
        "iam:PassRole",
        "lambda:CreateFunction",
        "lambda:EnableReplication",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource",
        "route53:ChangeResourceRecordSets",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "s3:CreateBucket",
        "s3:GetAccelerateConfiguration",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutAccelerateConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutObject",
        "s3:PutBucketTagging",
        "s3:GetBucketTagging",
        "lambda:ListEventSourceMappings",
        "lambda:CreateEventSourceMapping",
        "iam:UpdateAssumeRolePolicy",
        "iam:DeleteRolePolicy",
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:SetQueueAttributes",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:UpdateApp",
        "amplify:UpdateBranch"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifySSRViewLogGroups",
      "Effect" : "Allow",
```

```
      "Action" : "logs:DescribeLogGroups",
      "Resource" : "arn:aws:logs:*:*:log-group:*"
    },
    {
      "Sid" : "AmplifySSRCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/amplify/*"
    },
    {
      "Sid" : "AmplifySSRPushLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/amplify/*:log-stream:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AdministratorAccess-AWSElasticBeanstalk

`AdministratorAccess-AWSElasticBeanstalk`adalah kebijakanAWS terkelola yang: Memberikan izin administratif akun. Secara eksplisit memungkinkan pengembang dan administrator untuk mendapatkan akses langsung ke sumber daya yang mereka butuhkan untuk mengelola aplikasiAWS Elastic Beanstalk

Menggunakan kebijakan ini

Anda dapat melampirkan`AdministratorAccess-AWSElasticBeanstalk` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 22 Januari 2021 19.36 UTC
- Waktu yang telah diedit: 23 Maret 2023, 23.45 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:Describe*",
        "acm:List*",
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "cloudformation:Estimate*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:Validate*",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "codecommit:Get*",
        "codecommit:UploadArchive",
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroup*",
```

```
        "ec2:CreateLaunchTemplate*",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteLaunchTemplate*",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroup*",
        "ecs:CreateCluster",
        "ecs:DeRegisterTaskDefinition",
        "ecs:Describe*",
        "ecs:List*",
        "ecs:RegisterTaskDefinition",
        "elasticbeanstalk:*",
        "elasticloadbalancing:Describe*",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "logs:Describe*",
        "rds:Describe*",
        "s3:ListAllMyBuckets",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:*"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CancelUpdateStack",
        "cloudformation:ContinueUpdateRollback",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:SignalResource",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:awseb-*",
        "arn:aws:cloudwatch:*:*:alarm:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:StartBuild"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/Elastic-Beanstalk-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "dynamodb:CreateTable",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable",
        "dynamodb:TagResource"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/awseb-e-*",
        "arn:aws:dynamodb:*:*:table/eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteCluster"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:*Rule",
        "elasticloadbalancing:*Tags",
        "elasticloadbalancing:SetRulePriorities",
        "elasticloadbalancing:SetSecurityGroups"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:*"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/eb-*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/eb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/*/awseb-*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/*/eb-*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/eb-*/*/*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-elasticbeanstalk*",
        "arn:aws:iam::*:instance-profile/aws-elasticbeanstalk*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk*",
      "Condition" : {
        "StringLike" : {
          "iam:PolicyArn" : [
            "arn:aws:iam::aws:policy/AWSElasticBeanstalk*",
            "arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalk*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/autoscaling.amazonaws.com/
AWSServiceRoleForAutoScaling*",
        "arn:aws:iam::*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk*",
```

```
        "arn:aws:iam::*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing*",
        "arn:aws:iam::*:role/aws-service-role/
managedupdates.elasticbeanstalk.amazonaws.com/AWSServiceRoleForElasticBeanstalk*",
        "arn:aws:iam::*:role/aws-service-role/
maintenance.elasticbeanstalk.amazonaws.com/AWSServiceRoleForElasticBeanstalk*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "elasticbeanstalk.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "managedupdates.elasticbeanstalk.amazonaws.com",
            "maintenance.elasticbeanstalk.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:*DBSubnetGroup",
        "rds:AuthorizeDBSecurityGroupIngress",
        "rds:CreateDBInstance",
        "rds:CreateDBSecurityGroup",
        "rds:DeleteDBInstance",
        "rds:DeleteDBSecurityGroup",
        "rds:ModifyDBInstance",
        "rds:RestoreDBInstanceFromDBSnapshot"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:secgrp:awseb-e-*",
        "arn:aws:rds:*:*:secgrp:eb-*",
```

```
        "arn:aws:rds:*:*:snapshot:*",
        "arn:aws:rds:*:*:subgrp:awseb-e-*",
        "arn:aws:rds:*:*:subgrp:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Delete*",
        "s3:Get*",
        "s3:Put*"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucket*",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:GetTopicAttributes",
        "sns:Publish",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:*QueueAttributes",
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:SendMessage",
```

```
        "sqs:TagQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:awseb-e-*",
        "arn:aws:sqs:*:*:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AlexaForBusinessDeviceSetup

`AlexaForBusinessDeviceSetup`adalah kebijakanAWS terkelola yang: Menyediakan akses pengaturan perangkat ke AlexaForBusiness layanan

Menggunakan kebijakan ini

Anda dapat melampirkan`AlexaForBusinessDeviceSetup` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 November 2017, 16:47 UTC
- Waktu yang telah diedit: 20 Mei 2019, 21.05 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:RegisterDevice",
        "a4b:CompleteRegistration",
        "a4b:SearchDevices",
        "a4b:SearchNetworkProfiles",
        "a4b:GetNetworkProfile",
        "a4b:PutDeviceSetupEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "A4bDeviceSetupAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:A4BNetworkProfile*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AlexaForBusinessFullAccess

`AlexaForBusinessFullAccess`adalah kebijakanAWS terkelola yang: Memberikan akses penuh ke AlexaForBusiness sumber daya dan akses ke terkaitLayanan AWS

Menggunakan kebijakan ini

Anda dapat melampirkan`AlexaForBusinessFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 November 2017, 16:47 UTC
- Waktu yang telah diedit: 01 Juli 2020, 21.01 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessFullAccess`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:*",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "*a4b.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*a4b.amazonaws.com/
AWSServiceRoleForAlexaForBusiness*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:A4B*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "A4B*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AlexaForBusinessGatewayExecution

`AlexaForBusinessGatewayExecution`adalah kebijakanAWS terkelola yang: Menyediakan akses eksekusi gateway ke AlexaForBusiness layanan

Menggunakan kebijakan ini

Anda dapat melampirkan`AlexaForBusinessGatewayExecution` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 November 2017, 16:47 UTC
- Waktu yang telah diedit: 30 November 2017 16.47 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:Send*",
        "a4b:Get*"
      ],
      "Resource" : "arn:aws:a4b:*:*:gateway/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:dd-*",
        "arn:aws:sqs:*:*:sd-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:List*",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AlexaForBusinessLifesizeDelegatedAccessPolicy

`AlexaForBusinessLifesizeDelegatedAccessPolicy`adalah kebijakanAWS terkelola yang: Menyediakan akses ke perangkat Lifesize AVS

Menggunakan kebijakan ini

Anda dapat melampirkan`AlexaForBusinessLifesizeDelegatedAccessPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 04 Juni 2020, 19:46 UTC
- Waktu yang telah diedit: 12 Juni 2020, 20.31 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:DisassociateDeviceFromRoom",
        "a4b:DeleteDevice",
        "a4b:UpdateDevice",
        "a4b:GetDevice"
      ],
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A2IWO7UEGWV4TL"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:RegisterAVSDevice"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "a4b:amazonId" : [
            "A2IWO7UEGWV4TL"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:SearchDevices"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
```

```
          "a4b:filters_deviceType" : [
            "*A2IWO7UEGWV4TL"
          ]
        },
        "Null" : {
          "a4b:filters_deviceType" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:AssociateDeviceWithRoom"
      ],
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A2IWO7UEGWV4TL",
        "arn:aws:a4b:us-east-1:*:room/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:GetRoom",
        "a4b:GetAddressBook",
        "a4b:SearchRooms",
        "a4b:CreateContact",
        "a4b:CreateRoom",
        "a4b:UpdateContact",
        "a4b:ListConferenceProviders",
        "a4b:DeleteRoom",
        "a4b:CreateAddressBook",
        "a4b:DisassociateContactFromAddressBook",
        "a4b:CreateConferenceProvider",
        "a4b:PutConferencePreference",
        "a4b:DeleteAddressBook",
        "a4b:AssociateContactWithAddressBook",
        "a4b:DeleteContact",
        "a4b:SearchProfiles",
        "a4b:UpdateProfile",
        "a4b:GetContact"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Action" : [
        "kms:DescribeKey"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AlexaForBusinessNetworkProfileServicePolicy

`AlexaForBusinessNetworkProfileServicePolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memungkinkan Alexa for Business untuk melakukan tugas otomatis yang dijadwalkan oleh profil jaringan Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 Maret 2019, 00:53 UTC
- Waktu yang telah diedit: 05 April 2019 09.57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "A4bPcaTagAccess",
      "Action" : [
        "acm-pca:GetCertificate",
        "acm-pca:IssueCertificate",
        "acm-pca:RevokeCertificate"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/a4b" : "enabled"
        }
      }
    },
    {
      "Sid" : "A4bNetworkProfileAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:A4BNetworkProfile*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AlexaForBusinessPolyDelegatedAccessPolicy

`AlexaForBusinessPolyDelegatedAccessPolicy`adalah kebijakanAWS terkelola yang: Menyediakan akses ke perangkat Poly AVS

Menggunakan kebijakan ini

Anda dapat melampirkan`AlexaForBusinessPolyDelegatedAccessPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 16 Oktober 2019, 19:48 UTC
- Waktu yang telah diedit: 16 Oktober 2019 19.48 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "a4b:DisassociateDeviceFromRoom",
        "a4b:DeleteDevice",
        "a4b:UpdateDevice",
        "a4b:GetDevice"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A238TWV36W3S92",
        "arn:aws:a4b:us-east-1:*:device/*/*:A1FUZ1SC53VJXD"
      ]
    },
    {
      "Action" : [
        "a4b:RegisterAVSDevice"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "a4b:amazonId" : [
            "A238TWV36W3S92",
            "A1FUZ1SC53VJXD"
          ]
        }
      }
    },
    {
      "Action" : [
        "a4b:SearchDevices"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "a4b:AssociateDeviceWithRoom"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A238TWV36W3S92",
        "arn:aws:a4b:us-east-1:*:device/*/*:A1FUZ1SC53VJXD",
        "arn:aws:a4b:us-east-1:*:room/*"
      ]
    },
    {
```

```
      "Action" : [
        "a4b:GetRoom",
        "a4b:SearchRooms",
        "a4b:CreateRoom",
        "a4b:GetProfile",
        "a4b:SearchSkillGroups",
        "a4b:DisassociateSkillGroupFromRoom",
        "a4b:AssociateSkillGroupWithRoom",
        "a4b:GetSkillGroup",
        "a4b:SearchProfiles",
        "a4b:GetAddressBook",
        "a4b:UpdateRoom"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AlexaForBusinessReadOnlyAccess

`AlexaForBusinessReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke AlexaForBusiness layanan

Menggunakan kebijakan ini

Anda dapat melampirkan`AlexaForBusinessReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 30 November 2017, 16:47 UTC
- Waktu yang telah diedit: 20 November 2019, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:Get*",
        "a4b:List*",
        "a4b:Search*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonAPIGatewayAdministrator

`AmazonAPIGatewayAdministrator`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh untuk membuat/mengedit/menghapus API di Amazon API Gateway melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonAPIGatewayAdministrator` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 Juli 2015, 17:34 UTC
- Waktu yang telah diedit: 09 Juli 2015 17.34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:*"
      ],
      "Resource" : "arn:aws:apigateway:*::/*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonAPIGatewayInvokeFullAccess

`AmazonAPIGatewayInvokeFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh untuk memanggil API di Amazon API Gateway.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonAPIGatewayInvokeFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 Juli 2015, 17:36 UTC
- Waktu yang telah diedit: 18 Desember 2018 08.25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : "arn:aws:execute-api:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonAPIGatewayPushToCloudWatchLogs

`AmazonAPIGatewayPushToCloudWatchLogs`adalah kebijakanAWS terkelola yang: Memungkinkan API Gateway untuk mendorong log ke akun pengguna.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonAPIGatewayPushToCloudWatchLogs` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 November 2015, 23:41 UTC

- Waktu yang telah diedit: 11 November 2015 23.41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:FilterLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonAppFlowFullAccess

`AmazonAppFlowFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon AppFlow dan akses keAWS layanan yang didukung sebagai sumber aliran atau tujuan (S3 dan Redshift). Juga menyediakan akses ke KMS untuk enkripsi

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonAppFlowFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 02 Juni 2020, 23:30 UTC
- Waktu yang telah diedit: 28 Pebruari 2022, 23.11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowFullAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "appflow:*",
      "Resource" : "*"
    },
    {
      "Sid" : "ListRolesForRedshift",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "KMSListAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "KMSListGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3PutBucketPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::appflow-*"
    },
    {
      "Sid" : "SecretsManagerCreateSecretAccess",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "appflow!*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPutResourcePolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        },
```

```
        "StringEqualsIgnoreCase" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appflow"
        }
      }
    },
    {
      "Sid" : "LambdaListFunctions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonAppFlowReadOnlyAccess

`AmazonAppFlowReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke alur Amazon Appflow

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonAppFlowReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 02 Juni 2020, 23:26 UTC
- Waktu yang telah diedit: 28 Februari 2022, 20.42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeConnector",
        "appflow:DescribeConnectors",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlows",
        "appflow:DescribeFlowExecution",
        "appflow:DescribeConnectorFields",
        "appflow:ListConnectors",
        "appflow:ListConnectorFields",
        "appflow:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonAppStreamFullAccess

`AmazonAppStreamFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon AppStream melaluiAWS Management Console.

Menggunakan kebijakan

Anda dapat melampirkan`AmazonAppStreamFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 28 Agustus 2020, 17.24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamFullAccess`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "appstream:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DescribeScalableTargets",
```

```
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:DeleteScheduledAction"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "iam:ListRoles",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/service-role/
ApplicationAutoScalingForAmazonAppStreamAccess",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com"
```

```
        }
      }
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appstream.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_AppStreamFleet",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "appstream.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonAppStreamPCAAccess

`AmazonAppStreamPCAAccess`adalah kebijakanAWS terkelola yang: Akses Amazon AppStream 2.0 keAWS Certificate Manager Private CA di akun pelanggan untuk autentikasi berbasis sertifikat

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonAppStreamPCAAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 24 Oktober 2022, 17:05 UTC
- Waktu yang telah diedit: 24 Oktober 2022, 17.05 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:*:acm-pca:*:*:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/euc-private-ca" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonAppStreamReadOnlyAccess

`AmazonAppStreamReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Amazon AppStream melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonAppStreamReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 07 Desember 2016 21.00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "appstream:Get*",
        "appstream:List*",
        "appstream:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonAppStreamServiceAccess

`AmazonAppStreamServiceAccess`adalah kebijakanAWS terkelola yang: Kebijakan default untuk peran AppStream layanan Amazon.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonAppStreamServiceAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 November 2016, 04:17 UTC
- Waktu yang telah diedit: 26 Juni 2020, 16.33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

Versi kebijakan

Versi kebijakan:v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints",
        "s3:ListAllMyBuckets",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::appstream2-36fb080bb8-*",
        "arn:aws:s3:::appstream-app-settings-*",
        "arn:aws:s3:::appstream-logs-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonAthenaFullAccess

`AmazonAthenaFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke Amazon Athena dan akses cakupan ke dependensi yang diperlukan untuk mengaktifkan kueri, menulis hasil, dan manajemen data.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonAthenaFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2016, 16:46 UTC
- Waktu yang telah diedit: 03 Januari 2024, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAthenaFullAccess`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "BaseAthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseGluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:StartColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseQueryResultsPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-athena-query-results-*"
      ]
    },
    {
      "Sid" : "BaseAthenaExamplesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::athena-examples*"
      ]
    },
    {
      "Sid" : "BaseS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseSNSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseCloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseDataZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:ListDomains",
        "datazone:ListProjects",
        "datazone:ListAccountEnvironments"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BasePricingPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "pricing:GetProducts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonAugmentedAIFullAccess

`AmazonAugmentedAIFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk melakukan semua operasi sumber daya Amazon Augmented AI, termasuk FlowDefinitions, HumanTaskUis dan HumanLoops. Tidak mengizinkan akses untuk membuat FlowDefinitions terhadap Workteam kerumunan publik.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonAugmentedAIFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 Desember 2019, 16:21 UTC
- Waktu yang telah diedit: 03 Desember 2019 08.21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops",
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions",
        "sagemaker:*HumanTaskUi",
        "sagemaker:*HumanTaskUis"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonAugmentedAIHumanLoopFullAccess

`AmazonAugmentedAIHumanLoopFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk melakukan semua operasi pada HumanLoops.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonAugmentedAIHumanLoopFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 Desember 2019, 16:20 UTC
- Waktu yang telah diedit: 03 Desember 2019 08.20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonAugmentedAIIntegratedAPIAccess

`AmazonAugmentedAIIntegratedAPIAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk melakukan semua operasi sumber daya Amazon Augmented AI, termasuk FlowDefinitions, HumanTaskUis dan HumanLoops. Juga menyediakan akses ke operasi layanan yang terintegrasi dengan Amazon Augmented AI.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonAugmentedAIIntegratedAPIAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 22 April 2020, 20:47 UTC
- Waktu yang telah diedit: 22 April 2020 20.47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops",
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions",
        "sagemaker:*HumanTaskUi",
        "sagemaker:*HumanTaskUis"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "textract:AnalyzeDocument"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rekognition:DetectModerationLabels"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonBedrockFullAccess

`AmazonBedrockFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke Amazon Bedrock serta akses terbatas ke layanan terkait yang diperlukan olehnya

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Desember 2023, 15:47 UTC
- Waktu telah diedit: 06 Desember 2023, 15:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAll",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:*:kms:*:::*"
    },
```

```
    {
      "Sid" : "APIsWithAllResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToBedrock",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonBedrock*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonBedrockReadOnly

`AmazonBedrockReadOnly`adalah kebijakan AWS terkelola yang: Menyediakan akses baca saja ke Amazon Bedrock

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonBedrockReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Desember 2023, 15:48 UTC
- Waktu telah diedit: 06 Desember 2023, 15:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockReadOnly`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetFoundationModel",
        "bedrock:ListFoundationModels",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:ListProvisionedModelThroughputs",
        "bedrock:GetModelCustomizationJob",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:ListCustomModels",
        "bedrock:GetCustomModel",
        "bedrock:ListTagsForResource",
        "bedrock:GetFoundationModelAvailability"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonBraketFullAccess

`AmazonBraketFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Braket melaluiAWS Management Console dan SDK. Juga menyediakan akses ke layanan terkait (misalnya, S3, log).

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonBraketFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Agustus 2020, 20:12 UTC
- Waktu yang telah diedit: 19 April 2023, 16.25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "servicequotas:GetServiceQuota",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/amazon-braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListNotebookInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StopNotebookInstance",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:ListTags",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
```

```
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance/amazon-braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/amazon-
braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "braket:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/braket.amazonaws.com/
AWSServiceRoleForAmazonBraket*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "braket.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonBraketServiceSageMakerNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonBraketJobsExecutionRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "braket.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "/aws/braket"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonBraketJobsExecutionPolicy

`AmazonBraketJobsExecutionPolicy`adalah kebijakanAWS terkelola yang: Memberikan akses keLayanan AWS dan sumber daya yang diperlukan untuk menjalankan Amazon Braket Job termasuk S3, Cloudwatch, IAM, dan Braket

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonBraketJobsExecutionPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 26 November 2021, 19:34 UTC
- Waktu yang telah diedit: 28 November 2021 05.34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/amazon-braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "braket:CancelJob",
        "braket:CancelQuantumTask",
        "braket:CreateJob",
        "braket:CreateQuantumTask",
        "braket:GetDevice",
        "braket:GetJob",
        "braket:GetQuantumTask",
```

```
        "braket:SearchDevices",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "braket:ListTagsForResource",
        "braket:TagResource",
        "braket:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonBraketJobsExecutionRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "braket.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
```

```
        "logs:CreateLogGroup",
        "logs:GetLogEvents",
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:StopQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "/aws/braket"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonBraketServiceRolePolicy

`AmazonBraketServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Amazon Braket membuat dan mengelolaAWS sumber daya atas nama Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, grup, grup, grup, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 04 Agustus 2020, 17:12 UTC
- Waktu yang telah diedit: 06 Agustus 2020, 20.10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket:*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonChimeFullAccess

`AmazonChimeFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Konsol Admin Amazon Chime melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonChimeFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 November 2017, 22:15 UTC
- Waktu yang telah diedit: 14 Desember 2020, 21.00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeFullAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Action" : [
        "chime:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:CreateQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Action" : [
        "kinesis:ListStreams"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/chime-chat-*",
        "arn:aws:kinesis:*:*:stream/chime-messaging-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::chime-chat-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonChimeReadOnly

`AmazonChimeReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Konsol Admin Amazon Chime melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonChimeReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 November 2017, 22:04 UTC
- Waktu yang telah diedit: 14 Desember 2020 20.53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

Versi kebijakan

Versi kebijakan:v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "chime:List*",
```

```
        "chime:Get*",
        "chime:Describe*",
        "chime:SearchAvailablePhoneNumbers"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonChimeSDK

`AmazonChimeSDK`adalah kebijakanAWS terkelola yang: Menyediakan akses ke operasi Amazon Chime SDK

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonChimeSDK` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 04 Februari 2020, 21:53 UTC
- Waktu yang telah diedit: 10 Januari 2023, 18.05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeSDK`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:CreateMeeting",
        "chime:CreateMeetingWithAttendees",
        "chime:DeleteMeeting",
        "chime:GetMeeting",
        "chime:ListMeetings",
        "chime:CreateAttendee",
        "chime:BatchCreateAttendee",
        "chime:DeleteAttendee",
        "chime:GetAttendee",
        "chime:ListAttendees",
        "chime:ListAttendeeTags",
        "chime:ListMeetingTags",
        "chime:ListTagsForResource",
        "chime:TagAttendee",
        "chime:TagMeeting",
        "chime:TagResource",
        "chime:UntagAttendee",
        "chime:UntagMeeting",
        "chime:UntagResource",
        "chime:StartMeetingTranscription",
        "chime:StopMeetingTranscription",
        "chime:CreateMediaCapturePipeline",
        "chime:CreateMediaConcatenationPipeline",
        "chime:CreateMediaLiveConnectorPipeline",
        "chime:DeleteMediaCapturePipeline",
        "chime:DeleteMediaPipeline",
        "chime:GetMediaCapturePipeline",
        "chime:GetMediaPipeline",
        "chime:ListMediaCapturePipelines",
        "chime:ListMediaPipelines"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

`AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`adalah kebijakan AWSterkelola yang: Kebijakan Terkelola Untuk Peran Tertaut Layanan Amazon Chime SDK MediaPipelines

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 04 April 2022, 22:02 UTC
- Waktu telah diedit: 08 Desember 2023, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutMetricsForChimeSDKNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/ChimeSDK"
        }
      }
    },
    {
      "Sid" : "AllowKinesisVideoStreamsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:UpdateDataRetention",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/ChimeMediaPipelines-*"
      ]
    },
    {
      "Sid" : "AllowKinesisVideoStreamsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "AllowChimeMeetingAccess",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetMeeting",
        "chime:CreateAttendee",
        "chime:DeleteAttendee"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonChimeSDKMessagingServiceRolePolicy

`AmazonChimeSDKMessagingServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Amazon Chime SDK Messaging mengaksesAWS sumber daya dan mengaktifkan fungsionalitas perpesanan

Menggunakan kebijakan ini kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, kebijakan ini, kebijakan ini, tidak dapat dilampirkan pada pengguna, kebijakan ini tidak dapat dilampirkan

detail kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 03 Maret 2023, 01:43 UTC
- Waktu yang telah diedit: 03 Maret 2023, 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan kebijakan kebijakan kebijakan ini adalah versi kebijakan default kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan ini adalah versi kebijakan default kebijakan kebijakan ini adalah versi kebijakan default kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON kebijakan JSON kebijakan JSON kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "kinesis.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/chime-messaging-*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonChimeServiceRolePolicy

`AmazonChimeServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan akses keAWS Sumber Daya yang digunakan atau dikelola oleh Amazon Chime

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau, atau peran.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 September 2019, 22:25 UTC
- Waktu yang telah diedit: 30 September 2019 07.25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/chime.amazonaws.com/
AWSServiceRoleForAmazonChime"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "chime.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonChimeTranscriptionServiceLinkedRolePolicy

`AmazonChimeTranscriptionServiceLinkedRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Amazon Chime mengakses Amazon Transcribe dan Amazon Transcribe Medical atas nama Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Kebijakan tidak dapat dilampirkan pada pengguna, grup, grup, grup, atau peran baru.

Rincian kebijakan terterterter

- Tipe: Kebijakan peran terkait layanan

- Waktu pembuatan: 04 Agustus 2021, 21:47 UTC
- Waktu yang telah diedit: 04 Agustus 2021 21.47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi standar adalah versi yang menentukan izin untuk kebijakan terterterterterterterterterterterterterterter. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:StartStreamTranscription",
        "transcribe:StartMedicalStreamTranscription"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonChimeUserManagement

`AmazonChimeUserManagement`adalah kebijakanAWS terkelola yang: Menyediakan akses manajemen pengguna ke Konsol Admin Amazon Chime melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonChimeUserManagement` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 November 2017, 22:17 UTC
- Waktu yang telah diedit: 18 Februari 2020, 19.26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeUserManagement`

Versi kebijakan

Versi kebijakan:v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "chime:ListAccounts",
        "chime:GetAccount",
        "chime:GetAccountSettings",
        "chime:UpdateAccountSettings",
        "chime:ListUsers",
        "chime:GetUser",
        "chime:GetUserByEmail",
        "chime:InviteUsers",
        "chime:InviteUsersFromProvider",
```

```
        "chime:SuspendUsers",
        "chime:ActivateUsers",
        "chime:UpdateUserLicenses",
        "chime:ResetPersonalPIN",
        "chime:LogoutUser",
        "chime:ListDomains",
        "chime:GetDomain",
        "chime:ListDirectories",
        "chime:ListGroups",
        "chime:SubmitSupportRequest",
        "chime:ListDelegates",
        "chime:ListAccountUsageReportData",
        "chime:GetMeetingDetail",
        "chime:ListMeetingEvents",
        "chime:ListMeetingsReportData",
        "chime:GetUserActivityReportData",
        "chime:UpdateUser",
        "chime:BatchUpdateUser",
        "chime:BatchSuspendUser",
        "chime:BatchUnsuspendUser",
        "chime:AssociatePhoneNumberWithUser",
        "chime:DisassociatePhoneNumberFromUser",
        "chime:GetPhoneNumber",
        "chime:ListPhoneNumbers",
        "chime:GetUserSettings",
        "chime:UpdateUserSettings",
        "chime:CreateUser",
        "chime:AssociateSigninDelegateGroupsWithAccount",
        "chime:DisassociateSigninDelegateGroupsFromAccount"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

`AmazonChimeVoiceConnectorServiceLinkedRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan terkelola untuk Peran Tertaut Layanan untuk Amazon Chime VoiceConnector

Menggunakan kebijakan

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 September 2019, 22:16 UTC
- Waktu yang telah diedit: 14 April 2023 21.49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan kebijakan kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JJJJJJJSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:GetVoiceConnector*"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:UpdateDataRetention",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/ChimeVoiceConnector-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:CreateMediaInsightsPipeline",
        "chime:GetMediaInsightsPipelineConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonCloudDirectoryFullAccess

`AmazonCloudDirectoryFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Cloud Directory Service.

Menggunakan kebijakan

Anda dapat melampirkan`AmazonCloudDirectoryFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 25 Februari 2017, 00:41 UTC
- Waktu yang telah diedit: 25 Februari 2017, 00:41 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "clouddirectory:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonCloudDirectoryReadOnlyAccess

`AmazonCloudDirectoryReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Amazon Cloud Directory Service.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCloudDirectoryReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 28 Februari 2017, 23:42 Februari 2017
- Waktu yang telah diedit: 28 Februari 2017 23.42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "clouddirectory:List*",
        "clouddirectory:Get*",
        "clouddirectory:LookupPolicy",
        "clouddirectory:BatchRead"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonCloudWatchEvidentlyFullAccess

`AmazonCloudWatchEvidentlyFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh hanya ke Amazon CloudWatch Terbukti. Juga menyediakan akses ke Amazon S3, Amazon SNS, Amazon CloudWatch, dan layanan terkait terkait lainnya.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCloudWatchEvidentlyFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan kebijakan kebijakan kebijakan kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 November 2021, 15:10 UTC
- Waktu yang telah diedit: 29 November 2021 15.10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "evidently:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchRUMEvidentlyRole-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:TagResource",
        "cloudwatch:UnTagResource"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:Evidently-Alarm-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "arn:*:sns:*:*:Evidently-*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonCloudWatchEvidentlyReadOnlyAccess

`AmazonCloudWatchEvidentlyReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Amazon CloudWatch Terbukti

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCloudWatchEvidentlyReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 November 2021, 15:08 UTC
- Waktu yang telah diedit: 29 November 2021 15.08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "evidently:GetExperiment",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonCloudWatchEvidentlyServiceRolePolicy

`AmazonCloudWatchEvidentlyServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Layanan CloudWatch Terbukti untuk mengelolaAWS Sumber Daya terkait atas nama pelanggan

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 September 2022, 17:25 UTC
- Waktu yang telah diedit: 13 September 2022, 17.25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "appconfig:StartDeployment",
      "Resource" : [
        "arn:aws:appconfig:*:*:application/*",
        "arn:aws:appconfig:*:*:deploymentstrategy/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeployedBy" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "appconfig:StartDeployment",
      "Resource" : "arn:aws:appconfig:*:*:application/*/configurationprofile/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/Owner" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "appconfig:TagResource",
      "Resource" : "arn:aws:appconfig:*:*:application/*/environment/*/deployment/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeployedBy" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "appconfig:StopDeployment",
      "Resource" : "arn:aws:appconfig:*:*:application/*"
    },
    {
      "Effect" : "Deny",
      "Action" : "appconfig:StopDeployment",
      "Resource" : "arn:aws:appconfig:*:*:application/*/environment/*/deployment/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/DeployedBy" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "appconfig:ListDeployments",
      "Resource" : "arn:aws:appconfig:*:*:application/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonCloudWatchRUMFullAccess

`AmazonCloudWatchRUMFullAccess`adalah kebijakanAWS terkelola yang: Memberikan izin akses penuh untuk layanan Amazon CloudWatch RUM

Menggunakan kebijakan

Anda dapat melampirkan`AmazonCloudWatchRUMFullAccess` ke pengguna, grup, dan peran Anda.

detail

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 November 2021, 15:46 UTC
- Waktu yang telah diedit: 29 November 2021 15.46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/rum.amazonaws.com/
AWSServiceRoleForRealUserMonitoring"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/RUM-Monitor*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
```

```
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:CreateIdentityPool",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:SetIdentityPoolRoles"
      ],
      "Resource" : "arn:aws:cognito-identity:*:*:identitypool/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy",
        "logs:CreateLogStream"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*RUMService*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group::log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:describeCanaries",
        "synthetics:describeCanariesLastRun"
      ],
      "Resource" : "arn:aws:synthetics:*:*:canary:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonCloudWatchRUMReadOnlyAccess

`AmazonCloudWatchRUMReadOnlyAccess`adalah kebijakanAWS terkelola yang: Memberikan izin hanya baca untuk layanan Amazon CloudWatch RUM

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCloudWatchRUMReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 29 November 2021, 15:43 UTC
- Waktu yang telah diedit: 28 Oktober 2022, 18.12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListRumMetricsDestinations",
        "rum:BatchGetRumMetricDefinitions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonCloudWatchRUMServiceRolePolicy

`AmazonCloudWatchRUMServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memberikan izin kepada Amazon CloudWatch RUM Service untuk mempublikasikan data pemantauan keAWS layanan terkait lainnya

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 November 2021, 23:17 UTC
- Waktu yang telah diedit: 22 Februari 2023, 20.35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "RUM/CustomMetrics/*",
            "AWS/RUM"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonCodeCatalystFullAccess

`AmazonCodeCatalystFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke AmazonCodeCatalyst

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCodeCatalystFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 20 April 2023, 16:50 UTC

- Waktu yang telah diedit: 20 April 2023, 16.50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeCatalystResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecatalyst:*",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeCatalystAssociateIAMRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "codecatalyst.amazonaws.com",
            "codecatalyst-runner.amazonaws.com"
          ]
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonCodeCatalystReadOnlyAccess

`AmazonCodeCatalystReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Amazon CodeCatalyst

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCodeCatalystReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 20 April 2023, 16:49 UTC
- Waktu yang telah diedit: 20 April 2023, 16.49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecatalyst:Get*",
        "codecatalyst:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonCodeCatalystSupportAccess

`AmazonCodeCatalystSupportAccess`adalah kebijakanAWS terkelola yang: Memungkinkan Amazon CodeCatalyst untuk membuat, memperbarui, dan menyelesaikanAWS Support kasus atas nama Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCodeCatalystSupportAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 April 2023, 12:34 UTC
- Waktu yang telah diedit: 20 April 2023, 12.34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeAttachment",
        "support:DescribeCaseAttributes",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:DescribeIssueTypes",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeSupportLevel",
        "support:SearchForCases",
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:InitiateCallForCase",
        "support:InitiateChatForCase",
        "support:PutCaseAttributes",
        "support:RateCaseCommunication",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonCodeGuruProfilerAgentAccess

`AmazonCodeGuruProfilerAgentAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses yang diperlukan oleh agen Amazon CodeGuru Profiler.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCodeGuruProfilerAgentAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 05 Februari 2021, 22:11 UTC
- Waktu yang telah diedit: 05 Mei 2022, 18.11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "codeguru-profiler:ConfigureAgent",
        "codeguru-profiler:CreateProfilingGroup",
        "codeguru-profiler:PostAgentProfile"
      ],
      "Resource" : "arn:aws:codeguru-profiler:*:*:profilingGroup/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonCodeGuruProfilerFullAccess

`AmazonCodeGuruProfilerFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon CodeGuru Profiler.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCodeGuruProfilerFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 Desember 2019, 10:13 UTC
- Waktu yang telah diedit: 15 Juli 2020, 03:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan kebijakan adalah versi yang menentukan izin kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeguru-profiler:*",
        "iam:ListRoles",
        "iam:ListUsers",
        "sns:ListTopics",
        "codeguru:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/*AWSServiceRoleForCodeGuruProfiler*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "codeguru-profiler.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonCodeGuruProfilerReadOnlyAccess

`AmazonCodeGuruProfilerReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Amazon CodeGuru Profiler.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCodeGuruProfilerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 Desember 2019, 10:30 UTC
- Waktu yang telah diedit: 27 Juni 2020, 23.52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeguru:Get*",
        "codeguru-profiler:BatchGet*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonCodeGuruReviewerFullAccess

`AmazonCodeGuruReviewerFullAccess`adalah kebijakanAWS terkelola yang: Memberikan akses penuh ke Amazon CodeGuru Reviewer dan akses scoped ke dependensi yang diperlukan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCodeGuruReviewerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 Desember 2019, 08:33 UTC
- Waktu yang telah diedit: 29 Agustus 2020, 04.16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:*",
        "codeguru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer"
    },
    {
      "Sid" : "CodeCommitAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CodeCommitTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:TagResource",
        "codecommit:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "codeguru-reviewer"
        }
      }
    },
    {
      "Sid" : "CodeConnectTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "codeguru-reviewer"
        }
      }
    },
    {
      "Sid" : "CodeConnectManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codestar-connections:ListConnections",
        "codestar-connections:PassConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "codestar-connections:ProviderAction" : [
            "ListRepositories",
            "ListOwners"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonCodeGuruReviewerReadOnlyAccess

`AmazonCodeGuruReviewerReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Amazon CodeGuru Reviewer.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCodeGuruReviewerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 Desember 2019, 08:48 UTC
- Waktu yang telah diedit: 29 Agustus 2020, 04.15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruReviewerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru:Get*",
        "codeguru-reviewer:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonCodeGuruReviewerServiceRolePolicy

`AmazonCodeGuruReviewerServiceRolePolicy`adalah kebijakanAWS terkelola yang: Peran terkait layanan yang diperlukan untuk Amazon CodeGuru Reviewer untuk mengakses sumber daya atas nama Anda.

Menggunakan

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan ke pengguna,,,,,,,,,,,,,,,,,,,,,,,,

Detail

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 03 Desember 2019, 05:31 UTC
- Waktu yang telah diedit: 27 November 2020, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

J

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessCodeGuruReviewerEnabledRepositories",
      "Effect" : "Allow",
```

```
      "Action" : [
        "codecommit:GetRepository",
        "codecommit:GetBranch",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetDifferences",
        "codecommit:GetPullRequest",
        "codecommit:ListPullRequests",
        "codecommit:PostCommentForPullRequest",
        "codecommit:GitPull",
        "codecommit:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/codeguru-reviewer" : "enabled"
        }
      }
    },
    {
      "Sid" : "AccessCodeGuruReviewerEnabledConnections",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "codestar-connections:ProviderAction" : [
            "ListBranches",
            "GetBranch",
            "ListRepositories",
            "ListOwners",
            "ListPullRequests",
            "GetPullRequest",
            "ListPullRequestComments",
            "ListPullRequestCommits",
            "ListCommitFiles",
            "ListBranchCommits",
            "CreatePullRequestDiffComment",
            "GitPull"
          ]
        },
        "Null" : {
```

```
          "aws:ResourceTag/codeguru-reviewer" : "false"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsResourceCleanup",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowGuruS3GetObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::codeguru-reviewer-*",
        "arn:aws:s3:::codeguru-reviewer-*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonCodeGuruSecurityFullAccess

`AmazonCodeGuruSecurityFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke AmazonCodeGuru Security.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCodeGuruSecurityFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 Mei 2023, 21:03 UTC
- Waktu yang telah diedit: 09 Mei 2023, 21.03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruSecurityFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonCodeGuruSecurityScanAccess

`AmazonCodeGuruSecurityScanAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses yang diperlukan untuk bekerja dengan pemindaian AmazonCodeGuru Security.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCodeGuruSecurityScanAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 Mei 2023, 20:54 UTC
- Waktu yang telah diedit: 09 Mei 2023, 20.54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruSecurityScanAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:CreateUploadUrl",
        "codeguru-security:GetScan",
        "codeguru-security:GetFindings"
      ],
      "Resource" : "arn:aws:codeguru-security:*:*:scans/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonCognitoDeveloperAuthenticatedIdentities

`AmazonCognitoDeveloperAuthenticatedIdentities`adalah kebijakanAWS terkelola yang: Menyediakan akses ke API Amazon Cognito untuk mendukung identitas terautentikasi pengembang dari backend autentikasi Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCognitoDeveloperAuthenticatedIdentities` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Maret 2015, 17:22 UTC
- Waktu yang telah diedit: 24 Maret 2015 07.22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:GetOpenIdTokenForDeveloperIdentity",
        "cognito-identity:LookupDeveloperIdentity",
        "cognito-identity:MergeDeveloperIdentities",
        "cognito-identity:UnlinkDeveloperIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonCognitoIdpEmailServiceRolePolicy

`AmazonCognitoIdpEmailServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan layanan Amazon Cognito User Pools untuk menggunakan identitas SES Anda untuk pengiriman email

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Maret 2019, 21:32 UTC
- Waktu yang telah diedit: 21 Maret 2019 09.32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ses:List*"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonCognitoIdpServiceRolePolicy

`AmazonCognitoIdpServiceRolePolicy`adalah kebijakanAWS terkelola yang: Mengaktifkan akses keLayanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon Cognito User Pools

Menggunakan kebijakan ini.

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, atau peran baru.

Rincian kebijakan kebijakan kebijakan kebijakan terkait kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 Juni 2020, 22:30 UTC
- Waktu yang telah diedit: 26 Juni 2020, 22.30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Kebijakan default default kebijakan default adalah versi yang menentukan izin untuk kebijakan default JP. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS

sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonCognitoPowerUser

`AmazonCognitoPowerUser`adalah kebijakanAWS terkelola yang: Menyediakan akses administratif ke sumber daya Amazon Cognito yang ada. Anda memerlukan hakAkun AWS admin untuk membuat sumber daya Cognito baru.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCognitoPowerUser` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Maret 2015, 17:14 UTC
- Waktu yang telah diedit: 01 Juni 2021 17.33 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonCognitoPowerUser`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:*",
        "cognito-idp:*",
        "cognito-sync:*",
        "iam:ListRoles",
        "iam:ListOpenIdConnectProviders",
        "iam:GetRole",
        "iam:ListSAMLProviders",
        "iam:GetSAMLProvider",
        "kinesis:ListStreams",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "sns:GetSMSSandboxAccountStatus",
        "sns:ListPlatformApplications",
        "ses:ListIdentities",
        "ses:GetIdentityVerificationAttributes",
        "mobiletargeting:GetApps",
        "acm:ListCertificates"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "cognito-idp.amazonaws.com",
            "email.cognito-idp.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/cognito-idp.amazonaws.com/
AWSServiceRoleForAmazonCognitoIdp*",
        "arn:aws:iam::*:role/aws-service-role/email.cognito-idp.amazonaws.com/
AWSServiceRoleForAmazonCognitoIdpEmail*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonCognitoReadOnly

`AmazonCognitoReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke sumber daya Amazon Cognito.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCognitoReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Maret 2015, 17:06 UTC
- Waktu yang telah diedit: 01 Agustus 2019, 19.21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoReadOnly`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:Describe*",
        "cognito-identity:Get*",
        "cognito-identity:List*",
        "cognito-idp:Describe*",
        "cognito-idp:AdminGet*",
        "cognito-idp:AdminList*",
        "cognito-idp:List*",
        "cognito-idp:Get*",
        "cognito-sync:Describe*",
        "cognito-sync:Get*",
        "cognito-sync:List*",
        "iam:ListOpenIdConnectProviders",
        "iam:ListRoles",
        "sns:ListPlatformApplications"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonCognitoUnAuthedIdentitiesSessionPolicy

`AmazonCognitoUnAuthedIdentitiesSessionPolicy`adalahAWSkebijakan terkelolathat: Kebijakan ini mendefinisikan kumpulan izin yang diizinkan untuk identitas yang tidak diautentikasi untuk Cognito Identity Pools. Kebijakan ini tidak dimaksudkan untuk digunakan sebagai kebijakan izin yang berdiri sendiri. Ini digunakan sebagai pagar pembatas terhadap kebijakan yang terlalu permisif yang dilampirkan untuk peran dalam kumpulan identitas. Jangan melampirkan kebijakan ini ke peran apa pun, karena Layanan Identitas Cognito akan secara otomatis memasukkannya sebagai kebijakan scoped down saat membuat kredensi. Hak istimewa untuk sementara mengakses lainnyaAWSsumber daya melalui alur yang disempurnakan sekarang akan ditentukan oleh persimpangan peran yang terkait dengan identitas pengguna yang tidak diautentikasi yang disediakan oleh layanan, dan hak istimewa yang diberikan dalam kebijakan terkelola yang dimiliki oleh Cognito ini.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCognitoUnAuthedIdentitiesSessionPolicy`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 19 Juli 2023, 23:04 UTC
- Waktu yang diedit:19 Juli 2023, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy`

Versi kebijakan

Versi kebijakan: v1(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:PutRumEvents",
        "sagemaker:InvokeEndpoint",
        "polly:*",
        "comprehend:*",
        "translate:*",
        "transcribe:*",
        "rekognition:*",
        "mobiletargeting:*",
        "firehose:*",
        "personalize:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonCognitoUnauthenticatedIdentities

`AmazonCognitoUnauthenticatedIdentities`adalah kebijakanAWS terkelola yang: Kebijakan ini mendefinisikan kumpulan izin yang diizinkan untuk identitas yang tidak diautentikasi untuk Pangkalan Identitas Cognito. Ini tidak perlu dilampirkan ke peran unauth Anda, karena Layanan Identitas Cognito akan secara otomatis memasukkannya sebagai kebijakan scoped down saat membuat kredensi. Hak istimewa untuk sementara mengaksesAWS sumber daya lain melalui alur yang ditingkatkan sekarang akan ditentukan oleh persimpangan peran yang terkait dengan identitas pengguna yang tidak diautentikasi yang disediakan oleh layanan, dan hak istimewa yang diberikan dalam kebijakan terkelola ini yang dimiliki oleh Cognito.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonCognitoUnauthenticatedIdentities` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Februari 2023, 22:36 UTC
- Waktu yang telah diedit: 01 Pebruari 2023, 22.36 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : "rum:PutRumEvents",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonConnect_FullAccess

`AmazonConnect_FullAccess`adalah kebijakanAWS terkelola yang: Tujuan kebijakan ini adalah untuk memberikan izin kepada penggunaAWS Connect yang diperlukan untuk menggunakan sumber daya Connect. Kebijakan ini menyediakan akses penuh ke sumber dayaAWS Connect melalui Connect Console dan API publik

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonConnect_FullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 20 November 2020, 19:54 UTC
- Waktu yang telah diedit: 07 Maret 2023, 14.49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnect_FullAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "connect:*",
        "ds:CreateAlias",
        "ds:AuthorizeApplication",
        "ds:CreateIdentityPoolDirectory",
        "ds:DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:UnauthorizeApplication",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lex:GetBots",
        "lex:ListBots",
        "lex:ListBotAliases",
        "logs:CreateLogGroup",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "lambda:ListFunctions",
        "ds:CheckAlias",
        "profile:ListAccountIntegrations",
        "profile:GetDomain",
        "profile:ListDomains",
        "profile:GetProfileObjectType",
        "profile:ListProfileObjectTypeTemplates"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "profile:AddProfileKey",
        "profile:CreateDomain",
        "profile:CreateProfile",
        "profile:DeleteDomain",
        "profile:DeleteIntegration",
        "profile:DeleteProfile",
        "profile:DeleteProfileKey",
        "profile:DeleteProfileObject",
        "profile:DeleteProfileObjectType",
        "profile:GetIntegration",
        "profile:GetMatches",
        "profile:GetProfileObjectType",
        "profile:ListIntegrations",
        "profile:ListProfileObjects",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "profile:MergeProfiles",
        "profile:PutIntegration",
        "profile:PutProfileObject",
        "profile:PutProfileObjectType",
        "profile:SearchProfiles",
        "profile:TagResource",
        "profile:UntagResource",
        "profile:UpdateDomain",
        "profile:UpdateProfile"
      ],
      "Resource" : "arn:aws:profile:*:*:domains/amazon-connect-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::amazon-connect-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "arn:aws:servicequotas:*:*:connect/*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "connect.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:DeleteServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/profile.amazonaws.com/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "profile.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonConnectCampaignsServiceLinkedRolePolicy

`AmazonConnectCampaignsServiceLinkedRolePolicy`adalah kebijakan AWS terkelola yang: Peran terkait layanan Kebijakan untuk Amazon Connect Campaigns

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 September 2021 20:54 UTC
- Waktu telah diedit: November 08, 2023, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "connect-campaigns:ListCampaigns"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "connect:BatchPutContact",
        "connect:StopContact"
      ],
```

```
      "Resource" : "arn:aws:connect:*:*:instance/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonConnectReadOnlyAccess

`AmazonConnectReadOnlyAccess`adalah kebijakanAWS terkelola yang: Memberikan izin untuk melihat instans Amazon Connect di instans AndaAkun AWS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonConnectReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 17 Oktober 2018, 21:00 UTC
- Waktu yang telah diedit: 06 November 2019, 22.10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "connect:Get*",
        "connect:Describe*",
        "connect:List*",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : "connect:GetFederationTokens",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonConnectServiceLinkedRolePolicy

`AmazonConnectServiceLinkedRolePolicy`adalah kebijakan AWS terkelola yang: Mengizinkan Amazon Connect membuat dan mengelola AWS sumber daya atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 07 September 2018, 00:21 UTC
- Waktu telah diedit: 28 November 2023, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect_*"
    },
    {
      "Sid" : "AllowS3ObjectForConnectBucket",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-connect-*/*"
      ]
    },
    {
      "Sid" : "AllowGetBucketMetadataForConnectBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-connect-*"
      ]
    },
    {
      "Sid" : "AllowConnectLogGroupAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/connect/*:*"
      ]
    },
    {
      "Sid" : "AllowListLexBotAccess",
      "Effect" : "Allow",
      "Action" : [
        "lex:ListBots",
        "lex:ListBotAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCustomerProfilesForConnectDomain",
```

```
      "Effect" : "Allow",
      "Action" : [
        "profile:SearchProfiles",
        "profile:CreateProfile",
        "profile:UpdateProfile",
        "profile:AddProfileKey",
        "profile:ListProfileObjectTypes",
        "profile:ListCalculatedAttributeDefinitions",
        "profile:ListCalculatedAttributesForProfile",
        "profile:GetDomain",
        "profile:ListIntegrations"
      ],
      "Resource" : "arn:aws:profile:*:*:domains/amazon-connect-*"
    },
    {
      "Sid" : "AllowReadPermissionForCustomerProfileObjects",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListProfileObjects",
        "profile:GetProfileObjectType"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/object-types/*"
      ]
    },
    {
      "Sid" : "AllowListIntegrationForCustomerProfile",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListAccountIntegrations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadForCustomerProfileObjectTemplates",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListProfileObjectTypeTemplates",
        "profile:GetProfileObjectTypeTemplate"
      ],
      "Resource" : "arn:aws:profile:*:*:/templates*"
    },
    {
      "Sid" : "AllowWisdomForConnectEnabledTaggedResources",
```

```
      "Effect" : "Allow",
      "Action" : [
        "wisdom:CreateContent",
        "wisdom:DeleteContent",
        "wisdom:CreateKnowledgeBase",
        "wisdom:GetAssistant",
        "wisdom:GetKnowledgeBase",
        "wisdom:GetContent",
        "wisdom:GetRecommendations",
        "wisdom:GetSession",
        "wisdom:NotifyRecommendationsReceived",
        "wisdom:QueryAssistant",
        "wisdom:StartContentUpload",
        "wisdom:UpdateContent",
        "wisdom:UntagResource",
        "wisdom:TagResource",
        "wisdom:CreateSession",
        "wisdom:CreateQuickResponse",
        "wisdom:GetQuickResponse",
        "wisdom:SearchQuickResponses",
        "wisdom:StartImportJob",
        "wisdom:GetImportJob",
        "wisdom:ListImportJobs",
        "wisdom:ListQuickResponses",
        "wisdom:UpdateQuickResponse",
        "wisdom:DeleteQuickResponse",
        "wisdom:PutFeedback"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowListOperationForWisdom",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:ListAssistants",
        "wisdom:ListKnowledgeBases"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowCustomerProfilesCalculatedAttributesForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:GetCalculatedAttributeForProfile",
        "profile:CreateCalculatedAttributeDefinition",
        "profile:DeleteCalculatedAttributeDefinition",
        "profile:GetCalculatedAttributeDefinition",
        "profile:UpdateCalculatedAttributeDefinition"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/calculated-attributes/*"
      ]
    },
    {
      "Sid" : "AllowPutMetricsForConnectNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Connect"
        }
      }
    },
    {
      "Sid" : "AllowSMSVoiceOperationsForConnect",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:SendTextMessage",
        "sms-voice:DescribePhoneNumbers"
      ],
      "Resource" : "arn:aws:sms-voice:*:*:phone-number/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonConnectSynchronizationServiceRolePolicy

`AmazonConnectSynchronizationServiceRolePolicy`adalah kebijakan AWS terkelola yang: Mengizinkan Amazon Connect menyinkronkan AWS sumber daya di seluruh wilayah atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 27 Oktober 2023, 22:38 UTC
- Waktu telah diedit: 27 Oktober 2023, 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:CreateUser*",
        "connect:UpdateUser*",
        "connect:DeleteUser*",
        "connect:DescribeUser*",
        "connect:ListUser*",
        "connect:CreateRoutingProfile",
        "connect:UpdateRoutingProfile*",
        "connect:DeleteRoutingProfile",
        "connect:DescribeRoutingProfile",
        "connect:ListRoutingProfile*",
        "connect:CreateAgentStatus",
        "connect:UpdateAgentStatus",
        "connect:DescribeAgentStatus",
        "connect:ListAgentStatuses",
        "connect:CreateQuickConnect",
        "connect:UpdateQuickConnect*",
        "connect:DeleteQuickConnect",
        "connect:DescribeQuickConnect",
        "connect:ListQuickConnects",
        "connect:CreateHoursOfOperation",
        "connect:UpdateHoursOfOperation",
        "connect:DeleteHoursOfOperation",
        "connect:DescribeHoursOfOperation",
        "connect:ListHoursOfOperations",
        "connect:CreateQueue",
        "connect:UpdateQueue*",
        "connect:DeleteQueue",
        "connect:DescribeQueue",
        "connect:ListQueue*",
        "connect:CreatePrompt",
        "connect:UpdatePrompt",
        "connect:DeletePrompt",
        "connect:DescribePrompt",
        "connect:ListPrompts",
        "connect:GetPromptFile",
        "connect:CreateSecurityProfile",
        "connect:UpdateSecurityProfile",
        "connect:DeleteSecurityProfile",
        "connect:DescribeSecurityProfile",
```

```
        "connect:ListSecurityProfile*",
        "connect:CreateContactFlow*",
        "connect:UpdateContactFlow*",
        "connect:DeleteContactFlow*",
        "connect:DescribeContactFlow*",
        "connect:ListContactFlow*",
        "connect:BatchGetFlowAssociation",
        "connect:CreatePredefinedAttribute",
        "connect:UpdatePredefinedAttribute",
        "connect:DeletePredefinedAttribute",
        "connect:DescribePredefinedAttribute",
        "connect:ListPredefinedAttributes",
        "connect:ListTagsForResource",
        "connect:TagResource",
        "connect:UntagResource",
        "connect:ListTrafficDistributionGroups",
        "connect:ListPhoneNumbersV2",
        "connect:UpdatePhoneNumber",
        "connect:DescribePhoneNumber",
        "connect:Associate*",
        "connect:Disassociate*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutMetricsForConnectNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Connect"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonConnectVoiceIDFullAccess

`AmazonConnectVoiceIDFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Connect Voice ID

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonConnectVoiceIDFullAccess` ke pengguna, grup, dan peran Anda.

Detail

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 26 September 2021, 19:04 UTC
- Waktu yang telah diedit: 26 September 2021 19.04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "voiceid:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonDataZoneDomainExecutionRolePolicy

`AmazonDataZoneDomainExecutionRolePolicy`adalah kebijakan AWS terkelola yang: Kebijakan default untuk peran DomainExecutionRole layanan Amazon DataZone. Peran ini digunakan oleh Amazon DataZone untuk membuat katalog, menemukan, mengatur, berbagi, dan menganalisis data dalam DataZone domain Amazon.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneDomainExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 27 September 2023, 21:55 UTC
- Waktu telah diedit: 12 Maret 2024, 23:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DomainExecutionRoleStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataSource",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataSource",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:GetAsset",
```

```
        "datazone:GetAssetType",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetListing",
        "datazone:GetProject",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListNotifications",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
        "datazone:Search",
```

```
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:UpdateDataSource",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest",
        "datazone:StartMetadataGenerationRun",
        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareStatement",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShareAssociations",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZoneEnvironmentRolePermissionsBoundary

`AmazonDataZoneEnvironmentRolePermissionsBoundary`adalah kebijakan AWS terkelola yang: Amazon DataZone membuat peran IAM untuk Lingkungan untuk melakukan tindakan analitik data, dan menggunakan kebijakan ini saat membuat peran ini untuk menentukan batas izinnya.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneEnvironmentRolePermissionsBoundary` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 September 2023, 23:38 UTC
- Waktu telah diedit: 17 November 2023, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateGlueConnection",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      }
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : [
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
```

```
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SameAccountKmsOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KmsOperationsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:Verify",
        "kms:Sign"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AnalyticsOperations",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*",
        "sqlworkbench:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QueryOperations",
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
```

```
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:Describe*",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
```

```
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:SearchTables",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeMetricFilters",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
```

```
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "secretsmanager:ListSecrets",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QueryOperationsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryResultsStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsManagerOperationsWithTagKeys",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AmazonDataZoneDomain" : "*",
          "aws:ResourceTag/AmazonDataZoneProject" : "*"
        },
```

```
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        }
      }
    },
    {
      "Sid" : "DataZoneS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/datazone/*"
      ]
    },
    {
      "Sid" : "DataZoneS3BucketLocation",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListDataZoneS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "*"
```

```
      ],
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "*/datazone/*",
            "datazone/*"
          ]
        }
      }
    },
    {
      "Sid" : "NotDeniedOperations",
      "Effect" : "Deny",
      "NotAction" : [
        "datazone:*",
        "sqlworkbench:*",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
```

```
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
```

```
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:List*",
        "iam:PassRole",
```

```
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ListKeys",
        "kms:Verify",
        "kms:Sign",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "s3:AbortMultipartUpload",
```

```
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:TagResource",
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZoneFullAccess

`AmazonDataZoneFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke Amazon DataZone melalui AWS Management Console serta akses terbatas ke layanan terkait yang diperlukan olehnya.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 September 2023, 20:06 UTC
- Waktu telah diedit: 12 Maret 2024, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
```

```
        "redshift-serverless:ListWorkgroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BucketReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "CreateBucketStatement",
      "Effect" : "Allow",
      "Action" : "s3:CreateBucket",
      "Resource" : "arn:aws:s3:::amazon-datazone*"
    },
    {
      "Sid" : "RamCreateResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RamResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
```

```
        "ram:RejectResourceShareInvitation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RamResourceReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd_*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd_*"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        }
      }
    },
    {
      "Sid" : "CreateSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd_*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZoneFullUserAccess

`AmazonDataZoneFullUserAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke Amazon DataZone, tetapi tidak mengizinkan pengelolaan domain, pengguna, atau akun terkait.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneFullUserAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 September 2023, 21:06 UTC
- Waktu telah diedit: 12 Maret 2024, 23:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneUserOperations",
      "Effect" : "Allow",
      "Action" : [
        "datazone:GetDomain",
        "datazone:CreateFormType",
        "datazone:GetFormType",
        "datazone:GetIamPortalLoginUrl",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
```

```
        "datazone:GetUserProfile",
        "datazone:GetGroupProfile",
        "datazone:ListGroupsForUser",
        "datazone:DeleteFormType",
        "datazone:CreateAssetType",
        "datazone:GetAssetType",
        "datazone:DeleteAssetType",
        "datazone:CreateGlossary",
        "datazone:GetGlossary",
        "datazone:DeleteGlossary",
        "datazone:UpdateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:GetGlossaryTerm",
        "datazone:DeleteGlossaryTerm",
        "datazone:UpdateGlossaryTerm",
        "datazone:CreateAsset",
        "datazone:GetAsset",
        "datazone:DeleteAsset",
        "datazone:CreateAssetRevision",
        "datazone:ListAssetRevisions",
        "datazone:AcceptPredictions",
        "datazone:RejectPredictions",
        "datazone:Search",
        "datazone:SearchTypes",
        "datazone:CreateListingChangeSet",
        "datazone:DeleteListing",
        "datazone:SearchListings",
        "datazone:GetListing",
        "datazone:CreateDataSource",
        "datazone:GetDataSource",
        "datazone:DeleteDataSource",
        "datazone:UpdateDataSource",
        "datazone:ListDataSources",
        "datazone:StartDataSourceRun",
        "datazone:GetDataSourceRun",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprint",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:ListEnvironmentBlueprints",
        "datazone:CreateProject",
```

```
        "datazone:UpdateProject",
        "datazone:GetProject",
        "datazone:DeleteProject",
        "datazone:ListProjects",
        "datazone:CreateProjectMembership",
        "datazone:DeleteProjectMembership",
        "datazone:ListProjectMemberships",
        "datazone:CreateEnvironmentProfile",
        "datazone:GetEnvironmentProfile",
        "datazone:UpdateEnvironmentProfile",
        "datazone:DeleteEnvironmentProfile",
        "datazone:ListEnvironmentProfiles",
        "datazone:CreateEnvironment",
        "datazone:GetEnvironment",
        "datazone:DeleteEnvironment",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:ListEnvironments",
        "datazone:ListAccountEnvironments",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetSubscriptionTarget",
        "datazone:DeleteSubscriptionTarget",
        "datazone:ListSubscriptionTargets",
        "datazone:CreateSubscriptionRequest",
        "datazone:AcceptSubscriptionRequest",
        "datazone:UpdateSubscriptionRequest",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectSubscriptionRequest",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:ListSubscriptionRequests",
        "datazone:DeleteSubscriptionRequest",
        "datazone:GetSubscription",
        "datazone:CancelSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:ListSubscriptions",
        "datazone:RevokeSubscription",
        "datazone:CreateSubscriptionGrant",
        "datazone:DeleteSubscriptionGrant",
        "datazone:GetSubscriptionGrant",
        "datazone:ListSubscriptionGrants",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:ListNotifications",
        "datazone:StartMetadataGenerationRun",
```

```
        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareOperations",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShareAssociations",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZoneGlueManageAccessRolePolicy

`AmazonDataZoneGlueManageAccessRolePolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin untuk mengizinkan Amazon mengaktifkan penerbitan dan akses hibah DataZone ke data.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneGlueManageAccessRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 September 2023, 20:21 UTC
- Waktu yang telah diedit: 14 Desember 2023, 23:03 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueTableDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:GetDatabases",
        "glue:GetTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LakeformationResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
```

```
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteLakeFormationOptIn",
        "lakeformation:GrantPermissions",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:ListPermissions",
        "lakeformation:RevokePermissions",
        "glue:GetDatabase",
        "glue:GetTable",
        "organizations:DescribeOrganization",
        "ram:GetResourceShareInvitations",
        "ram:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteResourcePolicy",
        "glue:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountLakeFormationResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
```

```
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceShareInvitationPermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share-invitation/*"
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DeleteResourceShare",
        "ram:DisassociateResourceShare",
        "ram:GetResourceShares",
        "ram:ListResourceSharePermissions",
        "ram:UpdateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:PermissionArn" : "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSDecryptPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/datazone:projectId" : "proj-all"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZonePortalFullAccessPolicy

`AmazonDataZonePortalFullAccessPolicy`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke DataZone API Amazon

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDataZonePortalFullAccessPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 26 Maret 2023, 18:24 UTC
- Waktu yang telah diedit: 26 Maret 2023, 18.24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "datazonecontrol:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonDataZonePreviewConsoleFullAccess

`AmazonDataZonePreviewConsoleFullAccess`adalah sebuahAWSkebijakan terkelolabahwa: Menyediakan akses penuh ke rilis Pratinjau AmazonDataZonemelaluiAWS Management Console. Juga menyediakan akses pilih ke layanan terkait lainnya.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDataZonePreviewConsoleFullAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 28 Maret 2023, 15:16 UTC
- Waktu yang diedit:13 Juli 2023, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v2(default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "datazonecontrol:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "glue:GetConnections",
        "glue:GetDatabase",
        "redshift:DescribeClusters",
        "ec2:DescribeSubnets",
        "secretsmanager:ListSecrets",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/AmazonDataZone-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneBootstrapServicePolicy-
AmazonDataZoneBootstrapRole",
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneServicePolicy-
AmazonDataZoneServiceRole"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZoneServiceRole*",
        "arn:aws:iam::*:role/service-role/AmazonDataZoneServiceRole*",
        "arn:aws:iam::*:role/AmazonDataZoneBootstrapRole*",
        "arn:aws:iam::*:role/service-role/AmazonDataZoneBootstrapRole",
        "arn:aws:iam::*:role/AmazonDataZoneDomainExecutionRole",
        "arn:aws:iam::*:role/service-role/AmazonDataZoneDomainExecutionRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazonecontrol.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai denganAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonDataZoneProjectDeploymentPermissionsBoundary

`AmazonDataZoneProjectDeploymentPermissionsBoundary`adalah kebijakanAWS terkelola yang: Amazon DataZone membuat peran IAM yang digunakannya untuk menerapkan proyek analisis data. DataZone menggunakan kebijakan ini saat membuat peran ini untuk menentukan batas izin mereka.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDataZoneProjectDeploymentPermissionsBoundary` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 21 Maret 2023, 02:54 UTC
- Waktu yang telah diedit: 04 April 2023, 02:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectDeploymentPermissionsBoundary`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
```

```
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*datazone*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneProjectRolePermissionsBoundary"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateKey",
        "kms:TagResource",
        "athena:CreateWorkGroup",
        "athena:TagResource",
        "iam:TagRole",
        "iam:TagPolicy",
        "logs:CreateLogGroup",
        "logs:TagLogGroup",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "datazone:*"
        },
        "StringLike" : {
          "aws:ResourceTag/datazone:projectId" : "proj-*"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup",
        "kms:ScheduleKeyDeletion",
        "kms:DescribeKey",
        "kms:EnableKeyRotation",
        "kms:DisableKeyRotation",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:Decrypt",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/datazone:projectId" : "proj-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "datazone:projectId"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
        "s3:DeleteBucket"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*",
        "arn:aws:s3:::datazone*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter*",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/*datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetRolePolicy",
        "iam:CreatePolicy",
        "iam:ListPolicyVersions",
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:ListPermissions",
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabases",
        "glue:GetDatabase",
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*datazone*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:DeleteBucketPolicy",
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketAcl",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging",
        "s3:PutBucketLogging",
        "s3:GetObject*",
        "s3:GetBucket*",
        "s3:List*",
        "s3:GetEncryptionConfiguration",
        "s3:DeleteObject*",
        "s3:PutObject*",
        "s3:Abort*"
      ],
      "Resource" : "arn:aws:s3:::*datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:Get*",
        "athena:List*",
        "ec2:CreateSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup",
        "ec2:Describe*",
        "ec2:Get*",
        "ec2:List*",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogGroups",
        "logs:DeleteLogGroup",
        "logs:DeleteRetentionPolicy"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:PutKeyPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.logs",
            "com.amazonaws.*.s3",
            "com.amazonaws.*.glue",
            "com.amazonaws.*.athena"
          ]
        }
      }
    },
    {
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeChangeSet",
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
```

```
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:TagResource",
        "cloudformation:GetTemplateSummary"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "s3:GetObject*",
        "s3:GetBucket*",
        "s3:List*",
        "s3:GetEncryptionConfiguration",
        "s3:DeleteObject*",
        "s3:PutObject*",
        "s3:Abort*",
        "s3:DeleteBucket"
      ],
      "NotResource" : [
        "arn:aws:s3:::*datazone*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "kms:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Deny",
      "NotAction" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
```

```
        "ssm:AddTagsToResource",
        "ssm:GetParameters",
        "ssm:GetParameter",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:DeleteBucketPolicy",
        "s3:CreateBucket",
        "s3:PutBucketAcl",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging",
        "s3:ListBucket",
        "s3:PutBucketLogging",
        "s3:DeleteBucket",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:CreatePolicy",
        "iam:ListPolicyVersions",
        "iam:DeletePolicy",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeChangeSet",
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:TagResource",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplateSummary",
        "athena:*",
        "kms:*",
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabases",
        "glue:GetDatabase",
        "lambda:*",
        "ec2:*",
        "logs:*",
        "servicecatalog:CreateApplication",
        "servicecatalog:DeleteApplication",
        "servicecatalog:GetApplication",
```

```
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy",
        "iam:UntagRole",
        "iam:PassRole",
        "iam:TagRole",
        "s3:GetBucket*",
        "s3:GetObject*",
        "s3:Abort*",
        "s3:GetEncryptionConfiguration",
        "s3:PutObject*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonDataZoneProjectRolePermissionsBoundary

`AmazonDataZoneProjectRolePermissionsBoundary`adalah kebijakanAWS terkelola yang: Amazon DataZone membuat peran IAM untuk proyek untuk melakukan tindakan analitik data, dan menggunakan kebijakan ini saat membuat peran ini untuk menentukan batas izin mereka.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDataZoneProjectRolePermissionsBoundary` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 21 Maret 2023, 02:51 UTC
- Waktu yang telah diedit: 21 Maret 2023, 02:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:List*",
        "s3:Get*",
        "s3:DeleteObjectVersion",
        "s3:RestoreObject",
        "s3:ReplicateObject",
```

```
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutObjectRetention",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:List*",
        "s3:Get*",
        "kms:List*",
        "kms:Get*",
        "kms:Describe*",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "logs:*",
        "athena:TerminateSession",
        "athena:CreatePreparedStatement",
        "athena:StopCalculationExecution",
        "athena:StartQueryExecution",
        "athena:UpdatePreparedStatement",
        "athena:BatchGet*",
```

```
        "athena:List*",
        "athena:UpdateNotebook",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:UpdateNotebookMetadata",
        "athena:DeleteNamedQuery",
        "athena:Get*",
        "athena:UpdateNamedQuery",
        "athena:CreateNamedQuery",
        "athena:ExportNotebook",
        "athena:StopQueryExecution",
        "athena:StartCalculationExecution",
        "athena:StartSession",
        "athena:CreatePresignedNotebookUrl",
        "athena:CreateNotebook",
        "athena:ImportNotebook",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "lakeformation:GetDataAccess",
        "lakeformation:BatchGrantPermissions",
        "lakeformation:GrantPermissions",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "ram:CreateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:AcceptResourceShareInvitation",
        "ram:Get*",
        "ram:List*",
        "redshift:DescribeClusters",
        "redshift:JoinGroup",
        "redshift:CreateClusterUser",
        "redshift:GetClusterCredentials",
        "redshift-data:*",
        "redshift:AuthorizeDataShare",
        "redshift:DescribeDataShares",
        "redshift:AssociateDataShareConsumer",
        "tag:GetResources",
        "iam:ListRoles",
```

```
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "glue:CreateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateDataQualityRuleset",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateWorkflow",
        "sqlworkbench:*",
        "datazone:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:List*",
        "kms:Get*",
        "kms:Describe*",
        "kms:Decrypt",
```

```
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:GenerateDataKey",
        "glue:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/datazone:projectId" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGet*",
        "glue:SearchTables",
        "glue:List*",
        "glue:Get*",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:PutResourcePolicy",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
```

```
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:UpdatePartition",
        "glue:NotifyEvent",
        "glue:DeleteResourcePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "NotAction" : [
        "s3:List*",
        "s3:Get*",
        "s3:Describe*",
        "s3:DeleteObjectVersion",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutObjectRetention",
        "s3:DeleteObject",
        "kms:List*",
        "kms:Get*",
        "kms:Describe*",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:GenerateDataKey",
        "ec2:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "logs:*",
        "athena:*",
        "glue:BatchGet*",
        "glue:Get*",
        "glue:SearchTables",
        "glue:List*",
        "glue:CreateDatabase",
```

```
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:PutResourcePolicy",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:UpdatePartition",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
```

```
        "glue:StartJobRun",
        "glue:CreateWorkflow",
        "glue:*DataQuality*",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:DeleteResourcePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "lakeformation:GetDataAccess",
        "lakeformation:BatchGrantPermissions",
        "lakeformation:GrantPermissions",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "ram:*",
        "redshift:*",
        "redshift-data:*",
        "tag:GetResources",
        "iam:List*",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:PassRole",
        "sqlworkbench:*",
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonDataZoneRedshiftGlueProvisioningPolicy

`AmazonDataZoneRedshiftGlueProvisioningPolicy`adalah kebijakan AWS terkelola yang: Amazon DataZone adalah layanan manajemen data yang memungkinkan Anda membuat katalog, menemukan, mengatur, berbagi, dan menganalisis data Anda. Dengan Amazon DataZone, Anda dapat berbagi dan mengakses data Anda di seluruh akun dan wilayah yang didukung. Amazon DataZone menyederhanakan pengalaman Anda di seluruh AWS layanan, termasuk, namun tidak terbatas pada, Amazon Redshift, Amazon Athena, AWS Glue, dan Lake Formation. AWS

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneRedshiftGlueProvisioningPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 September 2023, 20:19 UTC
- Waktu telah diedit: 12 Maret 2024, 16:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZonePermissionsToCreateEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
```

```
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneEnvironmentRolePermissionsBoundary",
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ],
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToManageCreatedEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:GetRole"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneCFStackCreationForEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneCFStackManagementForEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
      "Effect" : "Allow",
      "Action" : [
```

```
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:ListPermissions",
        "glue:CreateDatabase",
        "glue:GetDatabase",
        "athena:GetWorkGroup",
        "logs:DescribeLogGroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift:DescribeClusters",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentGlueDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteDatabase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentAthenaDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentAthenaResourceCreation",
      "Effect" : "Allow",
      "Action" : [
        "athena:CreateWorkGroup",
        "athena:TagResource",
        "iam:TagRole",
        "iam:TagPolicy",
        "logs:TagLogGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AmazonDataZoneEnvironmentLogGroupCreation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:datazone-*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLogGroupManagement",
      "Action" : [
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:datazone-*",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentIAMPolicyManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
        "iam:CreatePolicy",
        "iam:GetPolicy",
```

```
        "iam:ListPolicyVersions"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentS3ValidationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentKMSDecryptPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToTagAmazonDataZoneEnvironmentGlueResources",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToGetAmazonDataZoneEnvironmentBlueprintTemplates",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "RedshiftDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ListSchemas",
        "redshift-data:ExecuteStatement"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "DescribeStatementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "GetSecretValuePermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDataZoneRedshiftManageAccessRolePolicy

`AmazonDataZoneRedshiftManageAccessRolePolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan DataZone izin Amazon untuk mempublikasikan data Amazon Redshift ke katalog. Ini juga memberikan DataZone izin Amazon untuk memberikan akses atau mencabut akses ke Amazon Redshift atau Amazon Redshift Serverless aset yang diterbitkan dalam katalog.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDataZoneRedshiftManageAccessRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 September 2023, 20:15 UTC

- Waktu telah diedit: 16 November 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "redshiftDataScopeDownPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:ListTables",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift:*:*:cluster:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "listSecretsPermission",
      "Effect" : "Allow",
```

```
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "getWorkgroupPermission",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetWorkgroup",
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "getNamespacePermission",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetNamespace",
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "redshiftDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "dataSharesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare",
```

```
        "redshift:DescribeDataShares"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:datashare:*/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "associateDataShareConsumerPermission",
      "Effect" : "Allow",
      "Action" : "redshift:AssociateDataShareConsumer",
      "Resource" : "arn:aws:redshift:*:*:datashare:*/datazone*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDetectiveFullAccess

`AmazonDetectiveFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke layanan Amazon Detective dan akses scoped ke dependensi UI konsol

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDetectiveFullAccess` ke pengguna, grup, dan peran Anda.

Rincian Kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 April 2020, 17:57 UTC

- Waktu yang telah diedit: 17 Mei 2023, 19.39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveFullAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:*",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ArchiveFindings"
      ],
      "Resource" : "arn:aws:guardduty:*:*:detector/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "securityHub:GetFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonDetectiveInvestigatorAccess

`AmazonDetectiveInvestigatorAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penyidik ke layanan Detektif Amazon dan akses cakupan ke dependensi UI konsol. Kebijakan ini memberikan izin untuk menyelam ke Detektif untuk tujuan investigasi dan akses tulis terbatas ke Guardduty.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDetectiveInvestigatorAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Januari 2023, 15:24 UTC
- Waktu telah diedit: 27 November 2023, 03:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DetectivePermissions",
      "Effect" : "Allow",
      "Action" : [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
        "detective:GetGraphIngestState",
        "detective:GetMembers",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListDatasourcePackages",
        "detective:ListGraphs",
        "detective:ListHighDegreeEntities",
        "detective:ListInvitations",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "detective:SearchGraph",
        "detective:StartInvestigation",
        "detective:GetInvestigation",
        "detective:ListInvestigations",
        "detective:UpdateInvestigationState",
        "detective:ListIndicators",
        "detective:InvokeAssistant"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
```

```
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ArchiveFindings",
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "securityHub:GetFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonDetectiveMemberAccess

`AmazonDetectiveMemberAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses anggota ke layanan Amazon Detective dan akses scoped ke dependensi UI konsol.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDetectiveMemberAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 17 Januari 2023, 15:16 UTC
- Waktu yang telah diedit: 17 Januari 2023, 15.16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonDetectiveOrganizationsAccess

`AmazonDetectiveOrganizationsAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses Organizations untuk mengelola administrator yang didelegasikan untuk Amazon Detective dan akses scoped ke dependensi UI konsol. Ini juga memberikan izin untuk membuat peran yang berkaitan dengan layanan untuk Detective.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDetectiveOrganizationsAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 02 Maret 2023, 15:20 UTC
- Waktu yang telah diedit: 02 Maret 2023, 15.20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "detective:DisableOrganizationAdminAccount",
        "detective:EnableOrganizationAdminAccount",
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "detective.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "detective.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "detective.amazonaws.com",
            "guardduty.amazonaws.com",
            "macie.amazonaws.com",
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonDetectiveServiceLinkedRolePolicy

`AmazonDetectiveServiceLinkedRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Amazon Detective melakukan panggilan layanan atas nama Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, atau tidak dapat dilampirkan kebijakan ini ke pengguna, atau tidak dapat dilampirkan pada pengguna, atau

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 November 2021, 19.47 UTC
- Waktu yang telah diedit: 18 November 2021 19.47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan ini adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonDevOpsGuruConsoleFullAccess

`AmazonDevOpsGuruConsoleFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan akses penuh ke konsol DevOps Guru.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDevOpsGuruConsoleFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 17 Desember 2021, 18:43 UTC
- Waktu yang telah diedit: 25 Agustus 2022, 18.18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsListTopicsAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsTopicOperations",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:DevOps-Guru-*"
    },
    {
      "Sid" : "DevOpsGuruSlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "devops-guru.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "DevOpsGuruSlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    },
    {
      "Sid" : "RDSDescribeDBInstancesAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PerformanceInsightsMetricsDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics",
        "pi:DescribeDimensionKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsFilterLogEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonDevOpsGuruFullAccess

`AmazonDevOpsGuruFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon DevOps Guru.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDevOpsGuruFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Desember 2020, 16:38 UTC
- Waktu yang telah diedit: 25 Agustus 2022, 18.23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "DevOpsGuruFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsListTopicsAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsTopicOperations",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:DevOps-Guru-*"
```

```
    },
    {
      "Sid" : "DevOpsGuruSlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DevOpsGuruSlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    },
    {
      "Sid" : "RDSDescribeDBInstancesAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsFilterLogEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonDevOpsGuruOrganizationsAccess

`AmazonDevOpsGuruOrganizationsAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk mengaktifkan dan mengelola Amazon DevOps Guru dalam suatu organisasi.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDevOpsGuruOrganizationsAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 15 November 2021, 23:50 UTC
- Waktu yang telah diedit: 15 November 2021 02.50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeOrganizationOverview",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:SearchOrganizationInsights"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListRoots"
      ],
      "Resource" : "arn:aws:organizations::*:"
    },
    {
      "Sid" : "OrganizationsAdminDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "devops-guru.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonDevOpsGuruReadOnlyAccess

`AmazonDevOpsGuruReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Amazon DevOps Guru Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDevOpsGuruReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Desember 2020, 16:34 UTC
- Waktu yang telah diedit: 25 Agustus 2022, 18.11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:DescribeAccountHealth",
        "devops-guru:DescribeAccountOverview",
        "devops-guru:DescribeAnomaly",
        "devops-guru:DescribeEventSourcesConfig",
        "devops-guru:DescribeFeedback",
        "devops-guru:DescribeInsight",
        "devops-guru:DescribeResourceCollectionHealth",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetCostEstimation",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListAnomaliesForInsight",
        "devops-guru:ListEvents",
        "devops-guru:ListInsights",
        "devops-guru:ListAnomalousLogGroups",
        "devops-guru:ListMonitoredResources",
        "devops-guru:ListNotificationChannels",
        "devops-guru:ListRecommendations",
        "devops-guru:SearchInsights",
        "devops-guru:StartCostEstimation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSDescribeDBInstancesAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsFilterLogEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonDevOpsGuruServiceRolePolicy

`AmazonDevOpsGuruServiceRolePolicy`adalah kebijakanAWS terkelola yang: Peran terkait layanan yang diperlukan untuk Amazon DevOpsGuru untuk mengakses sumber daya Anda.

Menggunakan kebijakan ini atau atau atau atau atau atau

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian detail detail JJJSON

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 01 Desember 2020, 10:24 UTC
- Waktu yang telah diedit: 10 Januari 2023, 14.36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v9 (default)

Versi versi atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON SON SON SON SON SON SON SON SON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudtrail:LookupEvents",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:ListDashboards",
        "cloudwatch:GetDashboard",
        "cloudformation:GetTemplate",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListImports",
        "codedeploy:BatchGetDeployments",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:ListDeployments",
        "config:DescribeConfigurationRecorderStatus",
        "config:GetResourceConfigHistory",
        "events:ListRuleNamesByTarget",
        "xray:GetServiceGraph",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "pi:GetResourceMetrics",
        "tag:GetResources",
        "lambda:GetFunction",
        "lambda:GetFunctionConcurrency",
        "lambda:GetAccountSettings",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:ListAliases",
        "lambda:ListEventSourceMappings",
        "lambda:GetPolicy",
        "ec2:DescribeSubnets",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
```

```
        "sqs:GetQueueAttributes",
        "kinesis:DescribeStream",
        "kinesis:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeStream",
        "dynamodb:ListStreams",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeAccountAttributes",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "s3:GetBucketNotification",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketWebsite",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListStorageLensConfigurations",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListServiceQuotas"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutTargetsOnASpecificRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/DevOps-Guru-managed-*"
    },
    {
```

```
      "Sid" : "AllowCreateOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAddTagsToOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Sid" : "AllowAccessOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-GuruInsightSsmOpsItemRelated" : "true"
        }
      }
    },
    {
      "Sid" : "AllowCreateManagedRule",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
    },
    {
      "Sid" : "AllowAccessManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
    },
```

```
    {
      "Sid" : "AllowOtherOperationsOnManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowTagBasedFilterLogEvents",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAPIGatewayGetIntegrations",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/??????????",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonDMSCloudWatchLogsRole

`AmazonDMSCloudWatchLogsRole`adalah kebijakan AWS terkelola yang: Menyediakan akses untuk mengunggah log replikasi DMS ke log cloudwatch di akun pelanggan.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDMSCloudWatchLogsRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Januari 2016, 23:44 UTC
- Waktu yang telah diedit: 23 Mei 2023, 21.32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribeOnAllLogGroups",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeOfAllLogStreamsOnDmsTasksLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*"
      ]
    },
    {
      "Sid" : "AllowCreationOfDmsLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:"
      ]
    },
    {
      "Sid" : "AllowCreationOfDmsLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-
serverless-*"
      ]
    },
    {
      "Sid" : "AllowUploadOfLogEventsToDmsLogStream",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-
serverless-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonDMSRedshiftS3Role

`AmazonDMSRedshiftS3Role`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk mengelola pengaturan S3 untuk titik akhir Redshift untuk DMS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDMSRedshiftS3Role` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 April 2016, 17:05 UTC
- Waktu yang telah diedit: 08 Juli 2019, 18.19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:DeleteBucket",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:GetBucketAcl",
        "s3:PutBucketVersioning",
        "s3:GetBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:DeleteBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::dms-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonDMSVPCManagementRole

`AmazonDMSVPCManagementRole`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk mengelola pengaturan VPC untuk konfigurasi pelanggan yangAWS dikelola

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDMSVPCManagementRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 18 November 2015, 16:33 UTC
- Waktu yang telah diedit: 23 Mei 2016 08.29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
```

```
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonDocDB-ElasticServiceRolePolicy

`AmazonDocDB-ElasticServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Amazon DocumentDB-Elastic mengelolaAWS sumber daya atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Kebijakan ini tidak dapat dilampirkan pada pengguna,,,,,,,,,,,,,,,,,,,,,,

Kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 November 2022, 14:17 UTC
- Waktu yang telah diedit: 30 November 2022, 14.17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan ini adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan dokumen kebijakan dokumen kebijakan dokumen kebijakan kebijakan dokumen kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB-Elastic"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonDocDBConsoleFullAccess

`AmazonDocDBConsoleFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh untuk mengelola Amazon DocumentDB dengan kompatibilitas MongoDB menggunakanAWS Management Console. Perhatikan kebijakan ini juga memberikan akses penuh untuk mempublikasikan semua topik SNS dalam akun, izin untuk membuat dan mengedit instans

Amazon EC2 dan konfigurasi VPC, izin untuk melihat dan mencantumkan kunci di Amazon KMS, dan akses penuh ke Amazon RDS dan Amazon Neptune.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDocDBConsoleFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 Januari 2019, 20:37 UTC
- Waktu yang telah diedit: 30 November 2022, 15.23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic:DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
```

```
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource",
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:CreateGlobalCluster",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DeleteGlobalCluster",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
```

```
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:ModifyGlobalCluster",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveFromGlobalCluster",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
```

```
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
```

```
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonDocDBElasticFullAccess

`AmazonDocDBElasticFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke Amazon DocumentDB Elastic Cluster dan izin lain yang diperlukan untuk dependensinya termasuk EC2, KMS, dan IAM. SecretsManager CloudWatch

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDocDBElasticFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Juni 2023, 13:51 UTC
- Waktu yang telah diedit: 21 Juni 2023, 18.05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic:DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
```

```
        "docdb-elastic:DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "kms:ViaService" : [
            "docdb-elastic.*.amazonaws.com"
          ],
          "aws:ResourceTag/DocDBElasticFullAccess" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/DocDBElasticFullAccess" : "*",
          "kms:ViaService" : [
            "docdb-elastic.*.amazonaws.com"
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:GetResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/DocDBElasticFullAccess" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonDocDBElasticReadOnlyAccess

`AmazonDocDBElasticReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya-baca ke Amazon DocDB-Elastic dan metrik. CloudWatch

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDocDBElasticReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 Juni 2023, 14:37 UTC
- Waktu yang telah diedit: 21 Juni 2023, 16.57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:ListClusters",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonDocDBFullAccess

`AmazonDocDBFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon DocumentDB dengan kompatibilitas MongoDB. Perhatikan kebijakan ini juga memberikan akses penuh untuk mempublikasikan semua topik SNS dalam akun dan akses penuh ke Amazon RDS dan Amazon Neptune.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDocDBFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 Januari 2019, 20:21 UTC
- Waktu yang telah diedit: 09 Januari 2019 08.21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
```

```
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
```

```
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonDocDBReadOnlyAccess

`AmazonDocDBReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke Amazon DocumentDB dengan kompatibilitas MongoDB. Perhatikan bahwa kebijakan ini juga memberikan akses ke sumber daya Amazon RDS dan Amazon Neptune.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDocDBReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 Januari 2019, 20:30 UTC
- Waktu yang telah diedit: 09 Januari 2019 20.30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventCategories",
```

```
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "kms:ListAliases",
        "kms:ListKeyPolicies"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "logs:DescribeLogStreams",
```

```
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonDRSVPCManagement

`AmazonDRSVPCManagement`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk mengelola pengaturan VPC untuk konfigurasi pelanggan yang dikelola Amazon

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDRSVPCManagement` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 02 September 2015, 00:09 UTC
- Waktu yang telah diedit: 02 September 2015 09.00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDRSVPCManagement`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonDynamoDBFullAccess

`AmazonDynamoDBFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon DynamoDB melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDynamoDBFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 29 Januari 2021 17.38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess`

Versi kebijakan

Versi kebijakan:v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "dynamodb:*",
        "dax:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
```

```
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:GetMetricData",
        "datapipeline:ActivatePipeline",
        "datapipeline:CreatePipeline",
        "datapipeline:DeletePipeline",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:PutPipelineDefinition",
        "datapipeline:QueryObjects",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes",
        "lambda:CreateFunction",
        "lambda:ListFunctions",
        "lambda:ListEventSourceMappings",
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping",
        "lambda:GetFunctionConfiguration",
        "lambda:DeleteFunction",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupQuery",
        "resource-groups:DeleteGroup",
```

```
        "resource-groups:CreateGroup",
        "tag:GetResources",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com",
            "application-autoscaling.amazonaws.com.cn",
            "dax.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "replication.dynamodb.amazonaws.com",
            "dax.amazonaws.com",
            "dynamodb.application-autoscaling.amazonaws.com",
            "contributorinsights.dynamodb.amazonaws.com",
            "kinesisreplication.dynamodb.amazonaws.com"
```

```
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonDynamoDBFullAccesswithDataPipeline

`AmazonDynamoDBFullAccesswithDataPipeline`adalah kebijakanAWS terkelola yang: Kebijakan ini berada di jalur pengusangan. Lihat dokumentasi untuk panduan: https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html. Menyediakan akses penuh ke Amazon DynamoDB termasuk Ekspor/Impor menggunakanAWS Data Pipeline melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonDynamoDBFullAccesswithDataPipeline` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 12 November 2015 02.17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "dynamodb:*",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsole"
    },
    {
      "Action" : [
        "lambda:*",
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsoleTriggers"
    },
    {
      "Action" : [
```

```
        "datapipeline:*",
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsoleImportExport"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRolePolicy",
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Sid" : "IAMEDPRoles"
    },
    {
      "Action" : [
        "ec2:CreateTags",
        "ec2:DescribeInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "elasticmapreduce:*",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "EMR"
    },
    {
      "Action" : [
        "s3:DeleteObject",
        "s3:Get*",
        "s3:List*",
        "s3:Put*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
```

```
      "Sid" : "S3"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonDynamoDBReadOnlyAccess

`AmazonDynamoDBReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses baca saja ke Amazon DynamoDB melalui. AWS Management Console

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonDynamoDBReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 20 Maret 2024, 15:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralReadOnlyAccess",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "dynamodb:GetItem",
        "dynamodb:GetResourcePolicy",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dax:Describe*",
        "dax:List*",
        "dax:GetItem",
        "dax:BatchGetItem",
        "dax:Query",
        "dax:Scan",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
```

```
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "lambda:ListFunctions",
        "lambda:ListEventSourceMappings",
        "lambda:GetFunctionConfiguration",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupQuery",
        "tag:GetResources",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CCIAccess",
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEBSCSIDriverPolicy

`AmazonEBSCSIDriverPolicy`adalah kebijakanAWS terkelola yang: kebijakan IAM yang memungkinkan akun layanan driver CSI untuk membuat panggilan ke layanan terkait seperti EC2 atas nama Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEBSCSIDriverPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 04 April 2022, 17:24 UTC
- Waktu yang telah diedit: 18 November 2022, 14.42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:ModifyVolume",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/CSIVolumeName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/kubernetes.io/created-for/pvc/name" : "*"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeSnapshotName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEC2ContainerRegistryFullAccess

`AmazonEC2ContainerRegistryFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses administratif ke sumber daya Amazon ECR

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEC2ContainerRegistryFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 21 Desember 2015, 17:06 UTC
- Waktu yang telah diedit: 05 Desember 2020, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:*",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "replication.ecr.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEC2ContainerRegistryPowerUser

`AmazonEC2ContainerRegistryPowerUser`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke repositori Amazon EC2 Container Registry, tetapi tidak mengizinkan penghapusan repositori atau perubahan kebijakan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEC2ContainerRegistryPowerUser` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 21 Desember 2015, 17:05 UTC
- Waktu yang telah diedit: 10 Desember 2019 20.48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEC2ContainerRegistryReadOnly

`AmazonEC2ContainerRegistryReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke repositori Amazon EC2 Container Registry.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEC2ContainerRegistryReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 21 Desember 2015, 17:04 UTC
- Waktu yang telah diedit: 10 Desember 2019 20.56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
```

```
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEC2ContainerServiceAutoscaleRole

`AmazonEC2ContainerServiceAutoscaleRole`adalah kebijakanAWS terkelola yang: Kebijakan untuk mengaktifkan Penskalaan Otomatis Tugas untuk Amazon EC2 Container Service

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEC2ContainerServiceAutoscaleRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 12 Mei 2016, 23:25 UTC
- Waktu yang telah diedit: 05 Februari 2018, 19.15 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEC2ContainerServiceEventsRole

`AmazonEC2ContainerServiceEventsRole`adalah kebijakanAWS terkelola yang: Kebijakan untuk mengaktifkan CloudWatch Acara untuk Layanan Kontainer EC2

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEC2ContainerServiceEventsRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 30 Mei 2017, 16:51 UTC
- Waktu yang diedit: 06 Maret 2023, 22.25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:RunTask"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ecs-tasks.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RunTask"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEC2ContainerServiceforEC2Role

`AmazonEC2ContainerServiceforEC2Role`adalah kebijakanAWS terkelola yang: Kebijakan default untuk Peran Amazon EC2 untuk Amazon EC2 Container Service.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEC2ContainerServiceforEC2Role` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Maret 2015, 18:45 UTC
- Waktu yang diedit: 06 Maret 2023, 22.19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`

Versi kebijakan

Versi kebijakan:v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags",
```

```
        "ecs:CreateCluster",
        "ecs:DeregisterContainerInstance",
        "ecs:DiscoverPollEndpoint",
        "ecs:Poll",
        "ecs:RegisterContainerInstance",
        "ecs:StartTelemetrySession",
        "ecs:UpdateContainerInstancesState",
        "ecs:Submit*",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterContainerInstance"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menentukan
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEC2ContainerServiceRole

`AmazonEC2ContainerServiceRole`adalah kebijakanAWS terkelola yang: Kebijakan default untuk peran layanan Amazon ECS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEC2ContainerServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 April 2015, 16:14 UTC
- Waktu yang telah diedit: 11 Agustus 2016 13.08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
```

```
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEC2FullAccess

`AmazonEC2FullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon EC2 melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEC2FullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 27 November 2018, 02:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "ec2:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "ec2scheduled.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "transitgateway.amazonaws.com"
          ]
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEC2ReadOnlyAccess

`AmazonEC2ReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses baca saja ke Amazon EC2 melalui. AWS Management Console

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEC2ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 14 Februari 2024, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEC2RoleforAWSCodeDeploy

`AmazonEC2RoleforAWSCodeDeploy`adalah kebijakanAWS terkelola yang: Menyediakan akses EC2 ke bucket S3 untuk mengunduh revisi. Peran ini diperlukan oleh CodeDeploy agen pada instans EC2.

Menggunakan kebijakan

Anda dapat melampirkan`AmazonEC2RoleforAWSCodeDeploy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Mei 2015, 18:10 UTC
- Waktu yang telah diedit: 20 Maret 2017 07.14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEC2RoleforAWSCodeDeployLimited

`AmazonEC2RoleforAWSCodeDeployLimited`adalah kebijakanAWS terkelola yang: Menyediakan akses terbatas EC2 ke bucket S3 untuk mengunduh revisi. Peran ini diperlukan oleh CodeDeploy agen pada instans EC2.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEC2RoleforAWSCodeDeployLimited` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu: 24 Agustus 2020, 17:55 UTC
- Waktu yang telah diedit: 20 Januari 2022, 21.37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEC2RoleforDataPipelineRole

`AmazonEC2RoleforDataPipelineRole`adalah kebijakanAWS terkelola yang: Kebijakan default untuk peran layanan Amazon EC2 Role for Data Pipeline.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEC2RoleforDataPipelineRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 22 Februari 2016 07.24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:*",
        "datapipeline:*",
        "dynamodb:*",
        "ec2:Describe*",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:ListInstance*",
        "elasticmapreduce:ModifyInstanceGroups",
        "rds:Describe*",
        "redshift:DescribeClusters",
```

```
        "redshift:DescribeClusterSecurityGroups",
        "s3:*",
        "sdb:*",
        "sns:*",
        "sqs:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEC2RoleforSSM

`AmazonEC2RoleforSSM`adalah kebijakanAWS terkelola yang: Kebijakan ini akan segera diusangkan. Gunakan AmazonsmManagedInstanceCore kebijakan untuk mengizinkan fungsi inti layananAWS Systems Manager pada instans EC2. Untuk informasi lebih lanjut lihat https:// docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile .html

Menggunakan kebijakan kebijakan ini

Anda dapat melampirkan`AmazonEC2RoleforSSM` ke pengguna, grup, dan peran Anda.

detail kebijakan kebijakan kebijakan kebijakan kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 29 Mei 2015, 17:48 UTC
- Waktu yang telah diedit: 24 Januari 2019 19.20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

Versi kebijakan

Versi kebijakan:v8 (default)

Versi default kebijakan kebijakan adalah versi yang menentukan izin kebijakan kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetEncryptionConfiguration",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEC2RolePolicyForLaunchWizard

`AmazonEC2RolePolicyForLaunchWizard`adalah kebijakanAWS terkelola yang: Kebijakan terkelola untuk peran LaunchWizard layanan Amazon untuk EC2

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEC2RolePolicyForLaunchWizard` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 13 November 2019, 08:05 UTC
- Waktu yang telah diedit: 16 Mei 2022, 21.16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard`

Versi kebijakan

Versi kebijakan:v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardResourceGroupID" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:ReplaceRoute"
      ],
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeRegions",
        "ec2:DescribeVolumes",
        "ec2:DescribeRouteTables",
        "ec2:ModifyInstanceAttribute",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricData",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LaunchWizardResourceGroupID",
            "LaunchWizardApplicationType"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:GetBucketLocation",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*",
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:Create*",
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "cloudformation:DescribeStackResources",
        "cloudformation:SignalResource",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "LaunchWizardResourceGroupID"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:PutItem",
        "sqs:ReceiveMessage",
```

```
        "sqs:SendMessage",
        "dynamodb:Scan",
        "s3:ListBucket",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteTable",
        "dynamodb:CreateTable",
        "s3:GetObject",
        "dynamodb:DescribeTable",
        "s3:GetBucketLocation",
        "dynamodb:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:dynamodb:*:*:table/LaunchWizard*",
        "arn:aws:sqs:*:*:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSSAP-InstallBackint"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:ListTagsForResource",
        "fsx:DescribeStorageVirtualMachines"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEC2SpotFleetAutoscaleRole

`AmazonEC2SpotFleetAutoscaleRole`adalah kebijakanAWS terkelola yang: Kebijakan untuk mengaktifkan Autoscaling untuk Amazon EC2 Spot Fleet

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEC2SpotFleetAutoscaleRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Agustus 2016, 18:27 UTC
- Waktu yang telah diedit: 18 Februari 2019, 19.17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ec2.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ec2.application-autoscaling.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEC2SpotFleetTaggingRole

`AmazonEC2SpotFleetTaggingRole`adalah kebijakanAWS terkelola yang: Memungkinkan Armada Spot EC2 untuk meminta, menghentikan, dan menandai Instans Spot atas nama Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEC2SpotFleetTaggingRole` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 29 Juni 2017, 18:19 UTC
- Waktu yang telah diedit: 23 April 2020 19.30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      },
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonECS_FullAccess

`AmazonECS_FullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses administratif ke sumber daya Amazon ECS dan memungkinkan fitur ECS melalui akses ke sumber dayaAWS layanan lain, termasuk VPC, grup Auto Scaling, dan CloudFormation tumpukan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonECS_FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 07 November 2017, 21:36 UTC
- Waktu yang telah diedit: 04 Januari 2023, 16:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECS_FullAccess`

Versi kebijakan

Versi kebijakan:v20 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:ListMeshes",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:Describe*",
        "autoscaling:UpdateAutoScalingGroup",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStack*",
        "cloudformation:UpdateStack",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "codedeploy:BatchGetApplicationRevisions",
```

```
        "codedeploy:BatchGetApplications",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ContinueDeployment",
        "codedeploy:CreateApplication",
        "codedeploy:CreateDeployment",
        "codedeploy:CreateDeploymentGroup",
        "codedeploy:GetApplication",
        "codedeploy:GetApplicationRevision",
        "codedeploy:GetDeployment",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:GetDeploymentTarget",
        "codedeploy:ListApplicationRevisions",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentConfigs",
        "codedeploy:ListDeploymentGroups",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "codedeploy:RegisterApplicationRevision",
        "codedeploy:StopDeployment",
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CancelSpotFleetRequests",
        "ec2:CreateInternetGateway",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:Describe*",
        "ec2:DetachInternetGateway",
        "ec2:DisassociateRouteTable",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RequestSpotFleet",
        "ec2:RunInstances",
        "ecs:*",
        "elasticfilesystem:DescribeAccessPoints",
```

```
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget",
        "events:ListTargetsByRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "fsx:DescribeFileSystems",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRoles",
        "lambda:ListFunctions",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:FilterLogEvents",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "servicediscovery:CreatePrivateDnsNamespace",
        "servicediscovery:CreateService",
        "servicediscovery:DeleteService",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetOperation",
        "servicediscovery:GetService",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:UpdateService",
        "sns:ListTopics"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/aws/service/ecs*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteInternetGateway",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "EC2ContainerService-*"
        }
      }
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ecs-tasks.amazonaws.com"
        }
      }
    },
    {
      "Action" : "iam:PassRole",
```

```
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsInstanceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsAutoscaleRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com",
            "application-autoscaling.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "ecs.amazonaws.com",
            "ecs.application-autoscaling.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateTargetGroup",
            "CreateRule",
            "CreateListener",
            "CreateLoadBalancer"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerS

`AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`adalah kebijakan AWS terkelola yang: Menyediakan akses administratif ke Private Certificate Authority, AWS Secrets Manager, dan lainnya yang Layanan AWS diperlukan untuk mengelola fitur ECS Service Connect TLS atas nama Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Januari 2024, 20:08 UTC
- Waktu telah diedit: 19 Januari 2024, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "TagOnCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RotateTLSCertificateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecretVersionStage"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "ecs-sc",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthority",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:DescribeCertificateAuthority"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthorityForIssuingEndEntityCertificate",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true",
          "acm-pca:TemplateArn" : "arn:aws:acm-pca:::template/EndEntityCertificate/V1"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonECSInfrastructureRolePolicyForVolumes

`AmazonECSInfrastructureRolePolicyForVolumes`adalah kebijakan AWS terkelola yang: Menyediakan akses ke sumber daya AWS layanan lain yang diperlukan untuk mengelola volume yang terkait dengan beban kerja ECS atas nama Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonECSInfrastructureRolePolicyForVolumes` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 Januari 2024, 22:56 UTC
- Waktu yang telah diedit: 10 Januari 2024, 22:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "TagOnCreateVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVolume",
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeVolumesForLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageEBSVolumeLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManageVolumeAttachmentsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DeleteEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:ResourceTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin dengan hak istimewa paling sedikit

AmazonECSServiceRolePolicy

`AmazonECSServiceRolePolicy`adalah kebijakan AWS terkelola yang: Kebijakan untuk mengaktifkan Amazon ECS mengelola klaster Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 Oktober 2017, 01:18 UTC
- Waktu telah diedit: 04 Desember 2023, 19:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSTaskManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:Describe*",
        "ec2:DetachNetworkInterface",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:Get*",
```

```
        "route53:List*",
        "route53:UpdateHealthCheck",
        "servicediscovery:DeregisterInstance",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:UpdateInstanceCustomHealthStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingManagement",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:SetInstanceProtection",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:PutLifecycleHook",
        "autoscaling:DeleteLifecycleHook",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:RecordLifecycleActionHeartbeat"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "autoscaling:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "AutoScalingPlanManagement",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling-plans:CreateScalingPlan",
        "autoscaling-plans:DeleteScalingPlan",
```

```
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:DescribeScalingPlanResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ecs-managed-*"
    },
    {
      "Sid" : "EventBridgeRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CWAlarmManagement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ECSTagging",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "CWLogGroupManagement",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*"
    },
    {
      "Sid" : "CWLogStreamManagement",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*:log-stream:*"
    },
    {
      "Sid" : "ExecuteCommandSessionManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExecuteCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*",
        "arn:aws:ssm:*:*:document/AmazonECS-ExecuteInteractiveCommand"
      ]
    },
    {
      "Sid" : "CloudMapResourceCreation",
      "Effect" : "Allow",
```

```
      "Action" : [
        "servicediscovery:CreateHttpNamespace",
        "servicediscovery:CreateService"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonECSManaged"
          ]
        }
      }
    },
    {
      "Sid" : "CloudMapResourceTagging",
      "Effect" : "Allow",
      "Action" : "servicediscovery:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonECSManaged" : "*"
        }
      }
    },
    {
      "Sid" : "CloudMapResourceDeletion",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DeleteService"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CloudMapResourceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonECSTaskExecutionRolePolicy

`AmazonECSTaskExecutionRolePolicy`adalah kebijakanAWS terkelola yang terkelola yang: Menyediakan akses ke sumber dayaAWS layanan lainnya yang diperlukan untuk menjalankan tugas Amazon ECS Amazon ECS

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonECSTaskExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 16 November 2017, 18:48 UTC
- Waktu yang telah diedit: 16 November 2017 18.48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan kebijakan yang menentukan izin untuk kebijakan yang ditentukan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEFSCSIDriverPolicy

`AmazonEFSCSIDriverPolicy`adalahAWSkebijakan terkelolabahwa: Menyediakan akses manajemen ke sumber daya EFS dan akses baca ke EC2

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEFSCSIDriverPolicy`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 25 Juli 2023, 20:10 UTC
- Waktu yang diedit:25 Juli 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy`

Versi kebijakan

Versi kebijakan: v1(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateAccessPoint",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateAccessPoint"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "efs.csi.aws.com/cluster"
```

```
        }
      }
    },
    {
      "Sid" : "AllowTagNewAccessPoints",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticfilesystem:CreateAction" : "CreateAccessPoint"
        },
        "Null" : {
          "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "efs.csi.aws.com/cluster"
        }
      }
    },
    {
      "Sid" : "AllowDeleteAccessPoint",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:DeleteAccessPoint",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/efs.csi.aws.com/cluster" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEKS_CNI_Policy

`AmazonEKS_CNI_Policy`adalah kebijakan AWS terkelola yang: Kebijakan ini menyediakan Plugin Amazon VPC CNI (amazon-vpc-cni-k8s) izin yang diperlukan untuk mengubah konfigurasi alamat IP pada node pekerja EKS Anda. Set izin ini memungkinkan CNI untuk membuat daftar, mendeskripsikan, dan memodifikasi Antarmuka Jaringan Elastis atas nama Anda. Informasi lebih lanjut tentang Plugin AWS VPC CNI tersedia di sini: https://github.com/aws/ 8s amazon-vpc-cni-k

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKS_CNI_Policy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2018, 21:07 UTC
- Waktu telah diedit: 04 Maret 2024, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSCNIPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
```

```
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEKSCNIPolicyENITag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEKSClusterPolicy

`AmazonEKSClusterPolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memberi Kubernetes izin yang diperlukan untuk mengelola sumber daya atas nama Anda. Kubernetes membutuhkan Ec2:CreateTags izin untuk menempatkan informasi identifikasi pada sumber daya EC2 termasuk namun tidak terbatas pada Instans, Grup Keamanan, dan Antarmuka Jaringan Elastis.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEKSClusterPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Mei 2018, 21:06 UTC
- Waktu yang telah diedit: 07 Pebruari 2023, 17.33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSClusterPolicy`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:UpdateAutoScalingGroup",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateRoute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteRoute",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DetachVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyVolume",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:AttachLoadBalancerToSubnets",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateLoadBalancerPolicy",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancerListeners",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DetachLoadBalancerFromSubnets",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
```

```
        "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEKSConnectorServiceRolePolicy

`AmazonEKSConnectorServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memungkinkan Amazon EKS untuk mengelolaAWS sumber daya untuk konektor EKS

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, peran baru.

Kebijakan

- Tipe: Kebijakan peran terkait layanan

- Waktu pembuatan: 04 September 2021, 20:31 UTC
- Waktu yang telah diedit: 04 September 2021 20.31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSConnectorServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Kebijakan ini adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessSSMService",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateActivation",
        "ssm:DescribeInstanceInformation",
        "ssm:DeleteActivation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConnectorAgentStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:ssm:*::document/AmazonEKS-ExecuteNonInteractiveCommand"
      ]
    },
    {
      "Sid" : "ConnectorAgentDeregister",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeregisterManagedInstance"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "PassAnyRoleToSsm",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PutManagedEventRule",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "eks-connector.amazonaws.com",
          "events:source" : "aws.ssm"
        }
      }
    },
    {
      "Sid" : "PutManagedEventTarget",
      "Effect" : "Allow",
      "Action" : "events:PutTargets",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "eks-connector.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEKSFargatePodExecutionRolePolicy

`AmazonEKSFargatePodExecutionRolePolicy`adalah kebijakanAWS terkelola bahwa: Menyediakan akses ke sumber dayaAWS layanan lainnya yang diperlukan untuk menjalankan pod-pod Amazon EKS diAWS Fargate

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEKSFargatePodExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 22 November 2019, 04:34 UTC
- Waktu yang telah diedit: 22 November 2019 04.34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEKSForFargateServiceRolePolicy

`AmazonEKSForFargateServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin yang diperlukan kepada Amazon EKS untuk menjalankan tugas terkelola

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 22 November 2019, 04:36 UTC
- Waktu yang telah diedit: 22 November 2019 04.36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSForFargateServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEKSLocalOutpostClusterPolicy

`AmazonEKSLocalOutpostClusterPolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin untuk instans kontrol-plane klaster lokal EKS yang berjalan di akun Anda untuk mengelola sumber daya atas nama Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEKSLocalOutpostClusterPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Agustus 2022, 21:56 UTC
- Waktu yang telah diedit: 17 Oktober 2022, 16.02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:DescribeInstanceProperties",
        "ssm:DescribeDocumentParameters",
        "ssm:ListInstanceAssociations",
        "ssm:RegisterManagedInstance",
        "ssm:UpdateInstanceInformation",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:PutComplianceItems",
        "ssm:PutInventory",
        "ecr-public:GetAuthorizationToken",
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/eks/*",
        "arn:aws:ecr:*:*:repository/bottlerocket-admin",
        "arn:aws:ecr:*:*:repository/bottlerocket-control-eks",
        "arn:aws:ecr:*:*:repository/diagnostics-collector-eks",
        "arn:aws:ecr:*:*:repository/kubelet-config-updater"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:*:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEKSLocalOutpostServiceRolePolicy

`AmazonEKSLocalOutpostServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Amazon EKS Local untuk memanggilAWS layanan atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Kebijakan ini tidak dapat dilampirkan pada pengguna, grup atau peran baru.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 Agustus 2022, 21:53 UTC
- Waktu yang telah diedit: 24 Oktober 2022, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcAttribute",
```

```
        "ec2:DescribePlacementGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
```

```
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*",
            "eks*"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "CreateSecurityGroup",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
```

```
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*",
            "eks*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:DeleteSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:DescribeSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks-local-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ssm:*::document/AmazonEKS-ControlPlaneInstanceProxy"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ResumeSession",
        "ssm:TerminateSession"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:GetOutpost"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEKSServicePolicy

`AmazonEKSServicePolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memungkinkan Amazon Elastic Container Service for Kubernetes untuk membuat dan mengelola sumber daya yang diperlukan guna mengoperasikan klaster EKS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEKSServicePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Mei 2018, 21:08 UTC
- Waktu yang telah diedit: 27 Mei 2020, 19.27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSServicePolicy`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "iam:ListAttachedRolePolicies",
        "eks:UpdateClusterVersion"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "route53:AssociateVPCWithHostedZone",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "eks.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEKSServiceRolePolicy

`AmazonEKSServiceRolePolicy`adalah kebijakanAWS terkelola yang: Peran Tertaut Layanan yang diperlukan untuk Amazon EKS untuk memanggilAWS layanan atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan pengguna Anda ke pengguna Anda.

Rincian terkelil terkelaskan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Februari 2020, 20:10 UTC
- Waktu yang telah diedit: 27 Mei 2020, 19.30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default adalah versi yang mengizinkan untuk kebijakan terkelil. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON SON SON SON SON SON SON SON SON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateNetworkInterfacePermission",
        "iam:ListAttachedRolePolicies",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "ec2:ResourceTag/Name" : "eks-cluster-sg*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ],
```

```
          "aws:RequestTag/Name" : "eks-cluster-sg*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "route53:AssociateVPCWithHostedZone",
      "Resource" : "arn:aws:route53:::hostedzone/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEKSVPCResourceController

`AmazonEKSVPCResourceController`adalah kebijakanAWS terkelola yang: Kebijakan yang digunakan oleh VPC Resource Controller untuk mengelola ENI dan IP untuk node pekerja.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEKSVPCResourceController` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 12 Agustus 2020, 00:55 UTC
- Waktu yang telah diedit: 12 Agustus 2020, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSVPCResourceController`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "ec2:ResourceTag/eks:eni:owner" : "eks-vpc-resource-controller"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DetachNetworkInterface",
```

```
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEKSWorkerNodePolicy

`AmazonEKSWorkerNodePolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini memungkinkan node pekerja Amazon EKS terhubung ke Amazon EKS Clusters.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonEKSWorkerNodePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2018, 21:09 UTC
- Waktu yang telah diedit: 27 November 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkerNodePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcs",
        "eks:DescribeCluster",
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElastiCacheFullAccess

`AmazonElastiCacheFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke Amazon ElastiCache melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElastiCacheFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 28 November 2023, 03:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : "elasticache:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/elasticache.amazonaws.com/
AWSServiceRoleForElastiCache",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticache.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateVPCEndpoints",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
        }
      }
    },
    {
      "Sid" : "AllowAccessToElastiCacheTaggedVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
    },
    {
      "Sid" : "TagVPCEndpointsOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAccessToEc2",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToAutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScalingActivities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "ListLogDeliveryStreams",
      "Effect" : "Allow",
      "Action" : [
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToOutposts",
      "Effect" : "Allow",
      "Action" : [
        "outposts:ListOutposts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToSNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElastiCacheReadOnlyAccess

`AmazonElastiCacheReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Amazon ElastiCache melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElastiCacheReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 08.40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticache:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonElasticContainerRegistryPublicFullAccess

`AmazonElasticContainerRegistryPublicFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses administratif ke sumber daya publik Amazon ECR

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticContainerRegistryPublicFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Desember 2020, 17:25 UTC
- Waktu yang telah diedit: 01 Desember 2020, 17.25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:*",
        "sts:GetServiceBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonElasticContainerRegistryPublicPowerUser

`AmazonElasticContainerRegistryPublicPowerUser`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke repositori Amazon ECR Public, tetapi tidak mengizinkan penghapusan repositori atau perubahan kebijakan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticContainerRegistryPublicPowerUser` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Desember 2020, 16:16 UTC
- Waktu yang telah diedit: 01 Desember 2020, 16.16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:DescribeRepositories",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:InitiateLayerUpload",
        "ecr-public:UploadLayerPart",
        "ecr-public:CompleteLayerUpload",
        "ecr-public:PutImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonElasticContainerRegistryPublicReadOnly

`AmazonElasticContainerRegistryPublicReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke repositori Amazon ECR Public.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticContainerRegistryPublicReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Desember 2020, 17:27 UTC
- Waktu yang telah diedit: 01 Desember 2020, 17.27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken",
        "ecr-public:BatchCheckLayerAvailability",
```

```
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:DescribeRepositories",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRegistryCatalogData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonElasticFileSystemClientFullAccess

`AmazonElasticFileSystemClientFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses klien root ke sistem file Amazon EFS

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticFileSystemClientFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 13 Januari 2020, 16:27 UTC
- Waktu yang telah diedit: 13 Januari 2020 08.27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonElasticFileSystemClientReadOnlyAccess

`AmazonElasticFileSystemClientReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses klien hanya baca ke sistem file Amazon EFS

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticFileSystemClientReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 13 Januari 2020, 16:24 UTC
- Waktu yang telah diedit: 13 Januari 2020 16.24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonElasticFileSystemClientReadWriteAccess

`AmazonElasticFileSystemClientReadWriteAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses klien baca dan tulis ke sistem file Amazon EFS

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticFileSystemClientReadWriteAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 13 Januari 2020, 16:21 UTC
- Waktu yang telah diedit: 13 Januari 2020, 16.21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonElasticFileSystemFullAccess

`AmazonElasticFileSystemFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke Amazon EFS melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonElasticFileSystemFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2015, 16:22 UTC
- Waktu telah diedit: 28 November 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricData",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:CreateTags",
        "elasticfilesystem:CreateAccessPoint",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "elasticfilesystem:DeleteTags",
        "elasticfilesystem:DeleteAccessPoint",
        "elasticfilesystem:DeleteFileSystemPolicy",
        "elasticfilesystem:DeleteReplicationConfiguration",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticfilesystem:DescribeAccessPoints",
```

```
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:ModifyMountTargetSecurityGroups",
        "elasticfilesystem:PutAccountPreferences",
        "elasticfilesystem:PutBackupPolicy",
        "elasticfilesystem:PutLifecycleConfiguration",
        "elasticfilesystem:PutFileSystemPolicy",
        "elasticfilesystem:UpdateFileSystem",
        "elasticfilesystem:UpdateFileSystemProtection",
        "elasticfilesystem:TagResource",
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:ListTagsForResource",
        "elasticfilesystem:Backup",
        "elasticfilesystem:Restore",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Sid" : "ElasticFileSystemFullAccess",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Sid" : "CreateServiceLinkedRoleForEFS",
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "elasticfilesystem.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticFileSystemReadOnlyAccess

`AmazonElasticFileSystemReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Amazon EFS melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticFileSystemReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Mei 2015, 16:25 UTC
- Waktu yang telah diedit: 10 Januari 2022, 18.53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricData",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:ListTagsForResource",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonElasticFileSystemServiceRolePolicy

`AmazonElasticFileSystemServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Amazon Elastic File System mengelolaAWS sumber daya atas nama Anda

Menggunakan

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan pada pengguna, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup

Policy details

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 November 2019, 16:52 UTC
- Waktu yang telah diedit: 10 Januari 2022, 19.27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:MountCapsule",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:ModifyNetworkInterfaceAttribute",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
```

```
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupVault",
        "backup:PutBackupVaultAccessPolicy"
      ],
      "Resource" : [
        "arn:aws:backup:*:*:backup-vault:aws/efs/automatic-backup-vault"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupPlan",
        "backup:CreateBackupSelection"
      ],
      "Resource" : [
        "arn:aws:backup:*:*:backup-plan:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/backup.amazonaws.com/
AWSServiceRoleForBackup"
```

```
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DeleteReplicationConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonElasticFileSystemsUtils

`AmazonElasticFileSystemsUtils`adalah kebijakanAWS terkelola yang: Memungkinkan pelanggan menggunakanAWS Systems Manager untuk secara otomatis mengelola paket utilitas (amazon-efs-utils) Amazon EFS pada instans EC2 mereka, dan gunakan CloudWatchLog untuk mendapatkan notifikasi keberhasilan/kegagalan pemasangan sistem file EFS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticFileSystemsUtils` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 29 September 2020, 15:16 UTC
- Waktu yang telah diedit: 29 September 2020 15.16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonElasticMapReduceEditorsRole

`AmazonElasticMapReduceEditorsRole`adalah kebijakanAWS terkelola yang: Kebijakan default untuk peran layanan Amazon Elastic MapReduce Editors.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticMapReduceEditorsRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 16 November 2018, 21:55 UTC
- Waktu yang telah diedit: 09 Pebruari 2023, 22.39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListSteps"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:elasticmapreduce:editor-id",
            "aws:elasticmapreduce:job-flow-id"
          ]
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonElasticMapReduceforAutoScalingRole

`AmazonElasticMapReduceforAutoScalingRole`adalah kebijakanAWS terkelola yang: Amazon Elastic MapReduce for Auto Scaling. Peran untuk memungkinkan Auto Scaling untuk menambah dan menghapus instance dari klaster EMR Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticMapReduceforAutoScalingRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 18 November 2016, 01:09 UTC
- Waktu yang telah diedit: 18 November 2016 01.09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonElasticMapReduceforEC2Role

`AmazonElasticMapReduceforEC2Role`adalah kebijakanAWS terkelola yang: Kebijakan default untuk peran layanan Amazon Elastic MapReduce for EC2.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticMapReduceforEC2Role` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC

- Waktu yang telah diedit: 11 Agustus 2017 23.57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan kebijakan adalah versi izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "cloudwatch:*",
        "dynamodb:*",
        "ec2:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSteps",
        "kinesis:CreateStream",
        "kinesis:DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:GetRecords",
        "kinesis:GetShardIterator",
        "kinesis:MergeShards",
        "kinesis:PutRecord",
        "kinesis:SplitShard",
        "rds:Describe*",
        "s3:*",
        "sdb:*",
```

```
        "sns:*",
        "sqs:*",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersions",
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:UpdatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:CreateUserDefinedFunction",
        "glue:UpdateUserDefinedFunction",
        "glue:DeleteUserDefinedFunction",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonElasticMapReduceFullAccess

`AmazonElasticMapReduceFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini berada di jalur pengusangan. Lihat dokumentasi untuk panduan: https://docs.aws.amazon.com/emr/latest/ManagementGuideemr-managed-iam-policies /.html. Menyediakan akses penuh ke Amazon Elastic MapReduce dan layanan dasar yang dibutuhkannya seperti EC2 dan S3

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticMapReduceFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 11 Oktober 2019 15.19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess`

Versi kebijakan

Versi kebijakan:v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
```

```
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateRoute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteRoute",
        "ec2:DeleteTags",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkAcls",
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "elasticmapreduce:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListRoles",
        "iam:PassRole",
        "kms:List*",
        "s3:*",
        "sdb:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "iam:AWSServiceName" : [
            "elasticmapreduce.amazonaws.com",
            "elasticmapreduce.amazonaws.com.cn"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonElasticMapReducePlacementGroupPolicy

`AmazonElasticMapReducePlacementGroupPolicy`adalah kebijakanAWS terkelola yang: Kebijakan untuk mengizinkan EMR membuat, menjelaskan, dan menghapus grup penempatan EC2.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticMapReducePlacementGroupPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 September 2020, 00:37 UTC
- Waktu yang telah diedit: 29 September 2020, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Resource" : "*",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeletePlacementGroup",
        "ec2:DescribePlacementGroups"
      ]
    },
    {
      "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonElasticMapReduceReadOnlyAccess

`AmazonElasticMapReduceReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Amazon Elastic MapReduce melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticMapReduceReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 29 Juli 2020, 23.14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
```

```
        "sdb:Select",
        "cloudwatch:GetMetricStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonElasticMapReduceRole

`AmazonElasticMapReduceRole`adalah kebijakanAWS terkelola yang: Kebijakan ini berada di jalur pengusangan. Lihat dokumentasi untuk panduan: https://docs.aws.amazon.com/emr/latest/ManagementGuideemr-managed-iam-policies /.html. Kebijakan default untuk peran MapReduce layanan Amazon Elastic.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticMapReduceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 24 Juni 2020, 22.24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

Versi kebijakan

Versi kebijakan:v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
```

```
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DeleteVolume",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:PassRole",
        "s3:CreateBucket",
        "s3:Get*",
        "s3:List*",
        "sdb:BatchPutAttributes",
        "sdb:Select",
        "sqs:CreateQueue",
        "sqs:Delete*",
        "sqs:GetQueue*",
        "sqs:PurgeQueue",
        "sqs:ReceiveMessage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:Describe*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot*",
```

```
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonElasticsearchServiceRolePolicy

`AmazonElasticsearchServiceRolePolicy`adalah kebijakan AWS terkelola yang: Izinkan Amazon Elasticsearch Service mengakses AWS layanan lain seperti EC2 Networking API atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 Juli 2017, 00:15 UTC
- Waktu telah diedit: 23 Oktober 2023, 06:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973135",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973136",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/ES"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973198",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973199",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973200",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "Stmt1480452973201",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973149",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973150",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973202",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonElasticTranscoder_FullAccess

`AmazonElasticTranscoder_FullAccess`adalah kebijakanAWS terkelola yang: Memberi pengguna akses penuh ke Elastic Transcoder dan akses ke layanan terkait yang diperlukan untuk fungsionalitas Elastic Transcoder penuh.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticTranscoder_FullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 April 2018, 18:59 UTC
- Waktu yang telah diedit: 10 Juni 2019 02.51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
```

```
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "elastictranscoder.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonElasticTranscoder_JobsSubmitter

`AmazonElasticTranscoder_JobsSubmitter`adalah kebijakanAWS terkelola yang: Memberikan izin kepada pengguna untuk mengubah preset, mengirimkan pekerjaan, dan melihat pengaturan Elastic Transcoder. Kebijakan ini juga memberikan beberapa akses hanya-baca ke beberapa layanan lain yang diperlukan untuk menggunakan konsol Elastic Transcode, termasuk S3, IAM, dan SNS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticTranscoder_JobsSubmitter` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 07 Juni 2018, 21:12 UTC
- Waktu yang telah diedit: 10 Juni 2019 02.50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "elastictranscoder:*Job",
        "elastictranscoder:*Preset",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonElasticTranscoder_ReadOnlyAccess

`AmazonElasticTranscoder_ReadOnlyAccess`adalah kebijakanAWS terkelola yang: Memberikan pengguna akses hanya-baca ke Elastic Transcoder dan daftar akses ke layanan terkait.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticTranscoder_ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 07 Juni 2018, 21:09 UTC
- Waktu yang telah diedit: 10 Juni 2019 02.48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
```

```
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonElasticTranscoderRole

`AmazonElasticTranscoderRole`adalah kebijakanAWS terkelola yang: Kebijakan default untuk peran layanan Amazon Elastic Transcoder.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonElasticTranscoderRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 13 Juni 2019 02.48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:Get*",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:*MultipartUpload*"
      ],
      "Sid" : "1",
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Sid" : "2",
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan izin identitas IAM
- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEMRCleanupPolicy

`AmazonEMRCleanupPolicy`adalah kebijakanAWS terkelola yang: Memungkinkan tindakan yang diperlukan EMR untuk mengakhiri dan menghapus sumber dayaAWS EC2 jika peran Layanan EMR telah kehilangan kemampuan itu.

Menggunakan kebijakan kebijakan kebijakan ini kebijakan kebijakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

detail kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 September 2017, 23:54 UTC
- Waktu yang telah diedit: 29 September 2020 21.11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi standar standar standar standar standar standar standar kebijakan default kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DeleteLaunchTemplate",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances",
        "ec2:CancelSpotInstanceRequests",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "ec2:DeleteVolume",
        "ec2:DescribePlacementGroups",
        "ec2:DeletePlacementGroup"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEMRContainersServiceRolePolicy

`AmazonEMRContainersServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan akses ke sumber dayaAWS layanan lain yang diperlukan untuk menjalankan Amazon EMR

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke peran Anda, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 09 Desember 2020, 00:38 UTC
- Waktu yang telah diedit: 10 Maret 2023, 22.58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:ListNodeGroups",
        "eks:DescribeNodeGroup",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
```

```
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ImportCertificate",
        "acm:AddTagsToCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/emr-container:endpoint:managed-certificate" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:DeleteCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/emr-container:endpoint:managed-certificate" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEMRFullAccessPolicy_v2

`AmazonEMRFullAccessPolicy_v2`adalahAWSkebijakan terkelolabahwa: Menyediakan akses penuh ke Amazon EMR

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEMRFullAccessPolicy_v2`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 12 Maret 2021, 01.50 UTC
- Waktu yang diedit:28 Juli 2023, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2`

Versi kebijakan

Versi kebijakan: v4(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunJobFlowExplicitlyWithEMRManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:RunJobFlow"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddInstanceFleet",
        "elasticmapreduce:AddInstanceGroups",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:CreateEditor",
        "elasticmapreduce:CreateSecurityConfiguration",
        "elasticmapreduce:DeleteEditor",
        "elasticmapreduce:DeleteSecurityConfiguration",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeEditor",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeReleaseLabel",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListEditors",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ModifyCluster",
        "elasticmapreduce:ModifyInstanceFleet",
        "elasticmapreduce:ModifyInstanceGroups",
        "elasticmapreduce:OpenEditorInConsole",
        "elasticmapreduce:PutAutoScalingPolicy",
        "elasticmapreduce:PutBlockPublicAccessConfiguration",
        "elasticmapreduce:PutManagedScalingPolicy",
        "elasticmapreduce:RemoveAutoScalingPolicy",
        "elasticmapreduce:RemoveManagedScalingPolicy",
        "elasticmapreduce:RemoveTags",
        "elasticmapreduce:SetTerminationProtection",
        "elasticmapreduce:StartEditor",
        "elasticmapreduce:StopEditor",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewMetricsInEMRConsole",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleForElasticMapReduce",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_DefaultRole_V2",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "elasticmapreduce.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForAutoScaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
        }
      }
    },
```

```
    {
      "Sid" : "ElasticMapReduceServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticmapreduce.amazonaws.com*/AWSServiceRoleForEMRCleanup*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "elasticmapreduce.amazonaws.com",
            "elasticmapreduce.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleUIActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "s3:ListAllMyBuckets",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM

- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEMRReadOnlyAccessPolicy_v2

`AmazonEMRReadOnlyAccessPolicy_v2`adalahAWSkebijakan terkelolabahwa: Menyediakan akses hanya baca ke Amazon EMR dan yang terkaitCloudWatchMetrik.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEMRReadOnlyAccessPolicy_v2`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 12 Maret 2021, 01:39 UTC
- Waktu yang diedit:02 Agustus 2023, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2`

Versi kebijakan

Versi kebijakan: v3(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
```

```
        "elasticmapreduce:DescribeEditor",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeReleaseLabel",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListEditors",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewMetricsInEMRConsole",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai denganAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEMRServerlessServiceRolePolicy

`AmazonEMRServerlessServiceRolePolicy`adalah kebijakan AWS terkelola yang: Mengizinkan akses ke sumber daya AWS layanan lain yang diperlukan untuk menjalankan Amazon EMRServerLess

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 Mei 2022, 23:15 UTC
- Waktu telah diedit: 25 Januari 2024, 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2PolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
```

```
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/EMRServerless",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonEMRServicePolicy_v2

`AmazonEMRServicePolicy_v2`adalah kebijakanAWS terkelola yang: Kebijakan ini digunakan untuk Peran Layanan Amazon EMR dan TIDAK boleh digunakan untuk pengguna atau peran IAM lainnya di akun Anda. Kebijakan ini memberikan izin untuk membuat dan mengelola sumber daya

yang terkait dengan EMR dan layanan terkait yang diperlukan untuk pengoperasian kluster EMR Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEMRServicePolicy_v2` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 12 Maret 2021
- Waktu yang telah diedit: 15 Pebruari 2022, 16.48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateInTaggedNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateWithEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRTaggedInstancesAndVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ResourcesToLaunchEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/ami-*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*:*:placement-group/EMR_*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:dedicated-host/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
    },
    {
      "Sid" : "ManageEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "ManageTagsOnEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaceNeededForPrivateSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateTaggedEMRResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:launch-template/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateFleet",
            "CreateLaunchTemplate",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "TagPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:placement-group/EMR_*"
      ]
    },
    {
      "Sid" : "ListActionsForEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDefaultSecurityGroupWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateDefaultSecurityGroupInVPCWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateDefaultSecurityGroupWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "ec2:CreateAction" : "CreateSecurityGroup"
```

```
        }
      }
    },
    {
      "Sid" : "ManageSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*"
    },
    {
      "Sid" : "DeletePlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeletePlacementGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
```

```
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupsForCapacityReservations",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*_EMR_Auto_Scaling"
    },
    {
      "Sid" : "PassRoleForAutoScaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonESCognitoAccess

`AmazonESCognitoAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses terbatas ke layanan konfigurasi Amazon Cognito.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonESCognitoAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 28 Februari 2018, 22:29 UTC
- Waktu yang telah diedit: 20 Desember 2021 14.04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESCognitoAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:UpdateUserPoolClient",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:AdminInitiateAuth",
        "cognito-idp:AdminUserGlobalSignOut",
        "cognito-idp:ListUserPoolClients",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:UpdateIdentityPool",
        "cognito-identity:SetIdentityPoolRoles",
        "cognito-identity:GetIdentityPoolRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com",
            "cognito-identity-us-gov.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonESFullAccess

`AmazonESFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke layanan konfigurasi Amazon ES.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonESFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Oktober 2015, 19:14 UTC
- Waktu yang telah diedit: 01 Oktober 2015 19.14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "es:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonESReadOnlyAccess

`AmazonESReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke layanan konfigurasi Amazon ES.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonESReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Oktober 2015, 19:18 UTC
- Waktu yang telah diedit: 03 Oktober 2018 03.32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Action" : [
        "es:Describe*",
        "es:List*",
        "es:Get*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEventBridgeApiDestinationsServiceRolePolicy

`AmazonEventBridgeApiDestinationsServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan EventBridge untuk mengakses sumber Secret Manager atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 11 Februari 2021, 20:52 UTC
- Waktu yang telah diedit: 11 Februari 2021 20.52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEventBridgeFullAccess

`AmazonEventBridgeFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon EventBridge.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEventBridgeFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Juli 2019, 14:08 UTC
- Waktu yang telah diedit: 01 Desember 2022, 17.00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
AmazonEventBridgeApiDestinationsServiceRolePolicy",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "apidestinations.events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "schemas.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccessForApiDestinations",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!*"
    },
    {
      "Sid" : "IAMPassRoleAccessForEventBridge",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "events.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "IAMPassRoleAccessForScheduler",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEventBridgePipesFullAccess

`AmazonEventBridgePipesFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon EventBridge Pipes.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEventBridgePipesFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Desember 2022, 17:03 UTC
- Waktu yang telah diedit: 01 Desember 2022, 17.03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgePipesActions",
      "Effect" : "Allow",
      "Action" : "pipes:*",
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEventBridgePipesOperatorAccess

`AmazonEventBridgePipesOperatorAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca dan operator (kemampuan untuk Menghentikan dan Mulai menjalankan Pipa) ke Amazon EventBridge Pipes.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEventBridgePipesOperatorAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Desember 2022, 17:04 UTC
- Waktu yang telah diedit: 01 Desember 2022, 17.04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEventBridgePipesReadOnlyAccess

`AmazonEventBridgePipesReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke Amazon EventBridge Pipes.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEventBridgePipesReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Desember 2022, 17:04 UTC
- Waktu yang telah diedit: 01 Desember 2022, 17.04 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEventBridgeReadOnlyAccess

`AmazonEventBridgeReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Amazon EventBridge.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEventBridgeReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Juli 2019, 13:59 UTC
- Waktu yang telah diedit: 01 Desember 2022, 17.02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DescribeEventBus",
        "events:DescribeEventSource",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:TestEventPattern",
        "events:DescribeArchive",
        "events:ListArchives",
```

```
        "events:DescribeReplay",
        "events:ListReplays",
        "events:DescribeConnection",
        "events:ListConnections",
        "events:DescribeApiDestination",
        "events:ListApiDestinations",
        "events:DescribeEndpoint",
        "events:ListEndpoints",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:ExportSchema",
        "schemas:GetCodeBindingSource",
        "schemas:GetDiscoveredSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "schemas:SearchSchemas",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEventBridgeSchedulerFullAccess

`AmazonEventBridgeSchedulerFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan yang AmazonEventBridgeSchedulerFullAccess dikelola memberikan izin untuk menggunakan semua tindakan EventBridge Penjadwal untuk jadwal, dan menjadwalkan grup.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEventBridgeSchedulerFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 10 November 2022, 18:37 UTC
- Waktu yang telah diedit: 10 November 2022, 18.37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "scheduler:*",
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEventBridgeSchedulerReadOnlyAccess

`AmazonEventBridgeSchedulerReadOnlyAccess`adalah kebijakanAWS terkelola yang: Kebijakan yang AmazonEventBridgeSchedulerReadOnlyAccess dikelola memberikan izin hanya-baca untuk melihat detail tentang jadwal Anda dan menjadwalkan grup

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEventBridgeSchedulerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 10 November 2022, 18:50 UTC
- Waktu yang telah diedit: 10 November 2022, 18.50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEventBridgeSchemasFullAccess

`AmazonEventBridgeSchemasFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon EventBridge Schemas.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEventBridgeSchemasFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 28 November 2019, 23:12 UTC
- Waktu yang telah diedit: 28 November 2019 23.12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEventBridgeSchemasFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "schemas:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEventBridgeManageRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
```

```
        "events:DisableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*Schemas*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonEventBridgeSchemasReadOnlyAccess

`AmazonEventBridgeSchemasReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Amazon EventBridge Schemas.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonEventBridgeSchemasReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 28 November 2019, 23:05 UTC
- Waktu yang telah diedit: 01 Mei 2020, 00:50 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEventBridgeSchemasReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "schemas:ListDiscoverers",
        "schemas:DescribeDiscoverer",
        "schemas:ListRegistries",
        "schemas:DescribeRegistry",
        "schemas:SearchSchemas",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:DescribeSchema",
        "schemas:GetDiscoveredSchema",
        "schemas:DescribeCodeBinding",
        "schemas:GetCodeBindingSource",
        "schemas:ListTagsForResource",
        "schemas:GetResourcePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonEventBridgeSchemasServiceRolePolicy

`AmazonEventBridgeSchemasServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memberikan izin ke Aturan Terkelola yang dibuat oleh EventBridge skema Amazon.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 27 November 2019, 01:10 UTC
- Waktu yang telah diedit: 27 November 2019, 01:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
        "events:DisableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/*Schemas-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonFISServiceRolePolicy

`AmazonFISServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan untuk memungkinkanAWS FIS mengelola pemantauan dan pemilihan sumber daya untuk eksperimen.

Menggunakan kebijakan

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan, atau peran.

Rincian

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Desember 2020, 21:18 UTC

- Waktu yang telah diedit: 25 Oktober 2022, 09:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v7 (default)

Versi default. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "fis.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventBridgeDescribe",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "Tagging",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmHistory"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeUserResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "iam:GetUser",
        "iam:GetRole",
        "iam:ListUsers",
        "iam:ListRoles",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "ecs:DescribeClusters",
        "ecs:DescribeTasks",
        "ecs:ListTasks",
        "eks:DescribeNodegroup",
        "eks:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonForecastFullAccess

`AmazonForecastFullAccess`adalah kebijakanAWS terkelola yang: Memberikan akses ke semua tindakan untuk Amazon Forecast

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonForecastFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 18 Januari 2019 01:52 UTC
- Waktu yang telah diedit: 18 Januari 2019 01.52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonForecastFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "forecast:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonFraudDetectorFullAccessPolicy

`AmazonFraudDetectorFullAccessPolicy`adalah kebijakanAWS terkelola yang: Memberikan akses ke semua tindakan untuk Amazon Fraud Detector

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonFraudDetectorFullAccessPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 Desember 2019, 22:46 UTC
- Waktu yang telah diedit: 03 Desember 2019 02.46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "frauddetector:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListEndpoints",
        "sagemaker:DescribeEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "frauddetector.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonFreeRTOSFullAccess

`AmazonFreeRTOSFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan Akses Penuh untuk Amazon FreeRTOS

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonFreeRTOSFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 November 2017 15:32 UTC
- Waktu yang telah diedit: 29 November 2017 15.32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "freertos:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonFreeRTOSOTAUpdate

`AmazonFreeRTOSOTAUpdate`adalah kebijakanAWS terkelola yang: Memungkinkan pengguna mengakses Pembaruan Amazon FreeRTOS OTA

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonFreeRTOSOTAUpdate` ke pengguna, grup, dan peran Anda.

Detail

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 27 Agustus 2018, 22:43 UTC
- Waktu yang telah diedit: 18 Desember 2020 17.47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::afr-ota*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "signer:StartSigningJob",
        "signer:DescribeSigningJob",
        "signer:GetSigningProfile",
        "signer:PutSigningProfile"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteJob",
        "iot:DescribeJob"
      ],
      "Resource" : "arn:aws:iot:*:*:job/AFR_OTA*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteStream"
      ],
      "Resource" : "arn:aws:iot:*:*:stream/AFR_OTA*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateStream",
        "iot:CreateJob"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan dan dan menghapus dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonFSxConsoleFullAccess

`AmazonFSxConsoleFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke Amazon FSx dan akses ke AWS layanan terkait melalui. AWS Management Console

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonFSxConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 16:36 UTC
- Waktu yang telah diedit: 10 Januari 2024, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListResourcesAssociatedWithFSxFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "kms:ListAliases",
        "logs:DescribeLogGroups",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx:CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
        "fsx:CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume",
        "fsx:CreateVolumeFromBackup",
        "fsx:DeleteBackup",
        "fsx:DeleteDataRepositoryAssociation",
        "fsx:DeleteFileCache",
        "fsx:DeleteFileSystem",
        "fsx:DeleteSnapshot",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume",
        "fsx:DescribeAssociatedFileGateways",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeDataRepositoryTasks",
        "fsx:DescribeFileCaches",
        "fsx:DescribeFileSystemAliases",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
```

```
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DisassociateFileGateway",
        "fsx:DisassociateFileSystemAliases",
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:ReleaseFileSystemNfsV3Locks",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:UpdateDataRepositoryAssociation",
        "fsx:UpdateFileCache",
        "fsx:UpdateFileSystem",
        "fsx:UpdateSharedVpcConfiguration",
        "fsx:UpdateSnapshot",
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateFSxSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSLRForLustreS3Integration",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "s3.data-source.lustre.fsx.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCrossAccountDataReplication",
      "Effect" : "Allow",
      "Action" : [
        "fsx:PutResourcePolicy",
        "fsx:GetResourcePolicy",
        "fsx:DeleteResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonFSxConsoleReadOnlyAccess

`AmazonFSxConsoleReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses baca saja ke Amazon FSx dan akses ke AWS layanan terkait melalui. AWS Management Console

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonFSxConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 16:35 UTC
- Waktu telah diedit: 10 Januari 2024, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FSxReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "fsx:Describe*",
        "fsx:ListTagsForResource",
        "kms:DescribeKey",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonFSxFullAccess

`AmazonFSxFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke Amazon FSx dan akses ke layanan terkaitAWS.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonFSxFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 16:34 UTC
- Waktu telah diedit: 10 Januari 2024, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxFullAccess`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ViewAWSDSDirectories",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx:CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
```

```
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
        "fsx:CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume",
        "fsx:CreateVolumeFromBackup",
        "fsx:DeleteBackup",
        "fsx:DeleteDataRepositoryAssociation",
        "fsx:DeleteFileCache",
        "fsx:DeleteFileSystem",
        "fsx:DeleteSnapshot",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume",
        "fsx:DescribeAssociatedFileGateways",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeDataRepositoryTasks",
        "fsx:DescribeFileCaches",
        "fsx:DescribeFileSystemAliases",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DisassociateFileGateway",
        "fsx:DisassociateFileSystemAliases",
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:ReleaseFileSystemNfsV3Locks",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:UpdateDataRepositoryAssociation",
        "fsx:UpdateFileCache",
        "fsx:UpdateFileSystem",
        "fsx:UpdateSharedVpcConfiguration",
        "fsx:UpdateSnapshot",
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CreateSLRForFSx",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSLRForLustreS3Integration",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "s3.data-source.lustre.fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateLogsForFSxWindowsAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/fsx/*"
      ]
    },
    {
      "Sid" : "WriteToAmazonKinesisDataFirehose",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord"
      ],
      "Resource" : [
```

```
        "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
      ]
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeEC2VpcResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCrossAccountDataReplication",
```

```
      "Effect" : "Allow",
      "Action" : [
        "fsx:PutResourcePolicy",
        "fsx:GetResourcePolicy",
        "fsx:DeleteResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonFSxReadOnlyAccess

`AmazonFSxReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Amazon FSx.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonFSxReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 28 November 2018, 16:33 UTC
- Waktu yang telah diedit: 28 November 2018 16.33 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:Describe*",
        "fsx:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonFSxServiceRolePolicy

`AmazonFSxServiceRolePolicy`adalah kebijakan AWS terkelola yang: Mengizinkan Amazon FSx mengelola AWS sumber daya atas nama Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 28 November 2018, 10:38 UTC
- Waktu yang telah diedit: 10 Januari 2024, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:GetAuthorizedApplicationDetails",
        "ds:UnauthorizeApplication",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAddresses",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:GetSecurityGroupsForVpc",
        "route53:AssociateVPCWithHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PutMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/FSx"
        }
      }
    },
    {
      "Sid" : "TagResourceNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "AmazonFSx.FileSystemId"
        }
      }
    },
    {
      "Sid" : "ManageNetworkInterface",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonFSx.FileSystemId" : "false"
        }
      }
    },
    {
      "Sid" : "ManageRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRoute",
        "ec2:ReplaceRoute",
        "ec2:DeleteRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonFSx" : "ManagedByAmazonFSx"
        }
      }
    },
    {
      "Sid" : "PutCloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/fsx/*"
    },
    {
      "Sid" : "ManageAuditLogs",
```

```
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonGlacierFullAccess

`AmazonGlacierFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Glacier melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonGlacierFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 08.40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "glacier:*",
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonGlacierReadOnlyAccess

`AmazonGlacierReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Amazon Glacier melaluiAWS Management Console.

Menggunakan kebijakan

Anda dapat melampirkan`AmazonGlacierReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 05 Mei 2016 18.46 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "glacier:DescribeJob",
        "glacier:DescribeVault",
        "glacier:GetDataRetrievalPolicy",
        "glacier:GetJobOutput",
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultLock",
        "glacier:GetVaultNotifications",
        "glacier:ListJobs",
        "glacier:ListMultipartUploads",
        "glacier:ListParts",
        "glacier:ListTagsForVault",
        "glacier:ListVaults"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonGrafanaAthenaAccess

`AmazonGrafanaAthenaAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan akses ke Amazon Athena dan dependensi yang diperlukan untuk mengaktifkan kueri dan menulis hasil ke s3 dari plugin Amazon Athena di Amazon Grafana.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonGrafanaAthenaAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 November 2021, 17:11 UTC
- Waktu yang telah diedit: 22 November 2021 07.11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
```

```
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetWorkGroup",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GrafanaDataSource" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::grafana-athena-query-results-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonGrafanaCloudWatchAccess

`AmazonGrafanaCloudWatchAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan akses ke Amazon CloudWatch dan dependensi yang diperlukan untuk digunakan CloudWatch sebagai sumber data dalam Amazon Managed Grafana.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonGrafanaCloudWatchAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 24 Maret 2023, 22:41 UTC
- Waktu yang telah diedit: 24 Maret 2023, 22.41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetInsightRuleReport"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:GetLogGroupFields",
        "logs:StartQuery",
        "logs:StopQuery",
```

```
        "logs:GetQueryResults",
        "logs:GetLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:ListSinks",
        "oam:ListAttachedLinks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonGrafanaRedshiftAccess

`AmazonGrafanaRedshiftAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan akses cakupan ke Amazon Redshift dan dependensi yang diperlukan untuk menggunakan plugin Amazon Redshift di Amazon Grafana.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonGrafanaRedshiftAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 November 2021, 23:15 UTC
- Waktu yang telah diedit: 26 November 2021 02.07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:ListTables",
        "redshift-data:ListSchemas"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GrafanaDataSource" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbname:*/*",
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "secretsmanager:ResourceTag/RedshiftQueryOwner" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonGrafanaServiceLinkedRolePolicy

`AmazonGrafanaServiceLinkedRolePolicy`adalah kebijakanAWS terkelola yang: Menyediakan akses keAWS Sumber Daya yang dikelola atau digunakan oleh Amazon Grafana.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 08 November 2022, 23:10 UTC
- Waktu yang telah diedit: 08 November 2022, 23.10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonGrafanaManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "Null" : {
          "aws:RequestTag/AmazonGrafanaManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AmazonGrafanaManaged" : "false"
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonGuardDutyFullAccess

`AmazonGuardDutyFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh untuk menggunakan Amazon GuardDuty.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonGuardDutyFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2017, 22:31 UTC
- Waktu telah diedit: 16 November 2023, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonGuardDutyFullAccessSid1",
      "Effect" : "Allow",
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ActionsForOrganizationsSid1",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamGetRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonGuardDutyMalwareProtectionServiceRolePolicy

`AmazonGuardDutyMalwareProtectionServiceRolePolicy`adalah kebijakan AWS terkelola yang: perlindungan GuardDuty malware menggunakan peran terkait layanan (SLR) bernama. AWSServiceRoleForAmazonGuardDutyMalwareProtection Peran terkait layanan ini memungkinkan perlindungan GuardDuty malware melakukan pemindaian tanpa agen untuk mendeteksi malware. Ini memungkinkan GuardDuty untuk membuat snapshot di akun Anda, dan berbagi snapshot dengan akun GuardDuty layanan untuk memindai malware. Ini mengevaluasi snapshot bersama ini dan menyertakan metadata instans EC2 yang diambil dalam temuan Perlindungan Malware. GuardDuty Peran AWSServiceRoleForAmazonGuardDutyMalwareProtection terkait layanan mempercayai layanan malware-protection.guardduty.amazonaws.com untuk mengambil peran tersebut.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 Juli 2022, 19:06 UTC
- Waktu telah diedit: 25 Januari 2024, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeAndListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTasks",
        "ecs:DescribeTasks",
        "eks:DescribeCluster"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSnapshotVolumeConditionalStatement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotConditionalStatement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
```

```
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyScanId"
        }
      }
    },
    {
      "Sid" : "CreateTagsPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:*/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
    },
    {
      "Sid" : "AddTagsToSnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/GuardDutyScanId" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "GuardDutyExcluded",
            "GuardDutyFindingDetected"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteAndShareSnapshotPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
```

```
        "StringLike" : {
          "ec2:ResourceTag/GuardDutyScanId" : "*"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "PreventPublicAccessToSnapshotPermission",
      "Effect" : "Deny",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/group" : "all"
        }
      }
    },
    {
      "Sid" : "CreateGrantPermission",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "snap-*"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "CreateGrant",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo",
            "RetireGrant",
            "DescribeKey"
          ]
        },
```

```
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "ShareSnapshotKMSPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeKeyPermission",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "GuardDutyLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
    },
    {
      "Sid" : "GuardDutyLogStreamPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
```

```
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
    },
    {
      "Sid" : "EBSDirectAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:GetSnapshotBlock",
        "ebs:ListSnapshotBlocks"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/GuardDutyScanId" : "*"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonGuardDutyReadOnlyAccess

`AmazonGuardDutyReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses baca saja ke GuardDuty sumber daya Amazon

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonGuardDutyReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2017, 22:29 UTC
- Waktu telah diedit: 16 November 2023, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:Describe*",
        "guardduty:Get*",
        "guardduty:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonGuardDutyServiceRolePolicy

`AmazonGuardDutyServiceRolePolicy`adalah kebijakan AWS terkelola yang: Aktifkan akses ke AWS Sumber Daya yang digunakan atau dikelola oleh Amazon Guard Duty

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 28 November 2017, 20:12 UTC
- Waktu telah diedit: 09 Februari 2024, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyGetDescribeListPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeTransitGatewayAttachments",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketTagging",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeSecurityGroups",
        "ecs:ListClusters",
        "ecs:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyCreateSLRPolicy",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateVpcEndpointPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        },
        "StringLike" : {
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.guardduty-data",
            "com.amazonaws.*.guardduty-data-fips"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyModifyDeleteVpcEndpointPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyManaged" : false
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutySecurityGroupManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyManaged" : false
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateSecurityGroupPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/GuardDutyManaged" : "*"
```

```
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateSecurityGroupForVpcPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateEksAddonPolicy",
      "Effect" : "Allow",
      "Action" : "eks:CreateAddon",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyEksAddonManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeleteAddon",
        "eks:UpdateAddon",
        "eks:DescribeAddon"
      ],
      "Resource" : "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
    },
```

```
    {
      "Sid" : "GuardDutyEksClusterTagResourcePolicy",
      "Effect" : "Allow",
      "Action" : "eks:TagResource",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyEcsPutAccountSettingsDefaultPolicy",
      "Effect" : "Allow",
      "Action" : "ecs:PutAccountSettingDefault",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:account-setting" : [
            "guardDutyActivate"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonHealthLakeFullAccess

`AmazonHealthLakeFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke HealthLake layanan Amazon.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonHealthLakeFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 17 Februari 2021, 01:07 UTC
- Waktu yang telah diedit: 17 Februari 2021 01.07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "healthlake:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "healthlake.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonHealthLakeReadOnlyAccess

`AmazonHealthLakeReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke HealthLake layanan Amazon.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonHealthLakeReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 17 Februari 2021, 02:43 UTC
- Waktu yang telah diedit: 17 Februari 2021 02.43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "healthlake:ListFHIRDatastores",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:DescribeFHIRExportJob",
        "healthlake:GetCapabilities",
        "healthlake:ReadResource",
        "healthlake:SearchWithGet",
        "healthlake:SearchWithPost"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonHoneycodeFullAccess

`AmazonHoneycodeFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Honeycode melaluiAWS Management Console dan SDK.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonHoneycodeFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Juni 2020, 20:28 UTC
- Waktu yang telah diedit: 24 Juni 2020, 20.28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:*"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonHoneycodeReadOnlyAccess

`AmazonHoneycodeReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Honeycode melaluiAWS Management Console dan SDK.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonHoneycodeReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Juni 2020, 20:28 UTC
- Waktu yang telah diedit: 01 Desember 2020, 17.27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:List*",
        "honeycode:Get*",
        "honeycode:Describe*",
        "honeycode:Query*"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menentukan
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonHoneycodeServiceRolePolicy

`AmazonHoneycodeServiceRolePolicy`adalah kebijakanAWS terkelola yang: Peran terkait layanan yang diperlukan untuk Amazon Honeycode untuk mengakses sumber daya Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 November 2020, 18:03 UTC
- Waktu yang telah diedit: 18 November 2020, 18.03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sso:GetManagedApplicationInstance"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonHoneycodeTeamAssociationFullAccess

`AmazonHoneycodeTeamAssociationFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Asosiasi Tim Honeycode melaluiAWS Management Console dan SDK.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonHoneycodeTeamAssociationFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Juni 2020, 20:28 UTC
- Waktu yang telah diedit: 24 Juni 2020, 20.28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:ListTeamAssociations",
        "honeycode:ApproveTeamAssociation",
        "honeycode:RejectTeamAssociation"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus menghapus identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonHoneycodeTeamAssociationReadOnlyAccess

`AmazonHoneycodeTeamAssociationReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Asosiasi Tim Honeycode melaluiAWS Management Console dan SDK.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonHoneycodeTeamAssociationReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Juni 2020, 20:27 UTC
- Waktu yang telah diedit: 24 Juni 2020, 20.27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:ListTeamAssociations"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonHoneycodeWorkbookFullAccess

`AmazonHoneycodeWorkbookFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Honeycode Workbook melaluiAWS Management Console dan SDK.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonHoneycodeWorkbookFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Juni 2020, 20:28 UTC
- Waktu yang telah diedit: 01 Desember 2020 17.30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:InvokeScreenAutomation",
        "honeycode:BatchCreateTableRows",
        "honeycode:BatchDeleteTableRows",
        "honeycode:BatchUpdateTableRows",
        "honeycode:BatchUpsertTableRows",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows",
        "honeycode:StartTableDataImportJob"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonHoneycodeWorkbookReadOnlyAccess

`AmazonHoneycodeWorkbookReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Buku Kerja Honeycode melaluiAWS Management Console dan SDK.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonHoneycodeWorkbookReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Juni 2020, 20:28 UTC
- Waktu yang telah diedit: 01 Desember 2020 17.32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonInspector2AgentlessServiceRolePolicy

`AmazonInspector2AgentlessServiceRolePolicy`adalah kebijakan AWS terkelola yang: Memberikan akses kepada Amazon Inspector yang diperlukan Layanan AWS untuk melakukan penilaian keamanan tanpa agen

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 November 2023, 15:18 UTC
- Waktu telah diedit: 20 November 2023, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstanceIdentification",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetSnapshotData",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InspectorScan" : "*"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAnyInstanceOrVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "DenyCreateSnapshotsOnExcludedInstances",
      "Effect" : "Deny",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/InspectorEc2Exclusion" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsOnAnySnapshotOnlyWithTag",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "InspectorScan"
        }
      }
    },
    {
      "Sid" : "CreateOnlyInspectorScanTagOnlyUsingCreateSnapshots",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : "CreateSnapshots"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "InspectorScan"
        }
      }
    },
    {
      "Sid" : "DeleteOnlySnapshotsTaggedForScanning",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/InspectorScan" : "*"
        }
      }
    },
    {
      "Sid" : "DenyKmsDecryptForExcludedKeys",
      "Effect" : "Deny",
      "Action" : "kms:Decrypt",
```

```
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/InspectorEc2Exclusion" : "true"
        }
      }
    },
    {
      "Sid" : "DecryptSnapshotBlocksVolContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "vol-*"
        }
      }
    },
    {
      "Sid" : "DecryptSnapshotBlocksSnapContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "snap-*"
        }
      }
    },
    {
      "Sid" : "DescribeKeysForEbsOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListKeyResourceTags",
      "Effect" : "Allow",
      "Action" : "kms:ListResourceTags",
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonInspector2FullAccess

`AmazonInspector2FullAccess`adalahAWSkebijakan terkelolabahwa: Menyediakan akses penuh ke Amazon Inspector dan akses ke layanan terkait lainnya seperti organisasi.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonInspector2FullAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 29 November 2021, 19.10 UTC
- Waktu yang diedit:03 Agustus 2023, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess`

Versi kebijakan

Versi kebijakan: v3(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "inspector2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
```

```
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonInspector2ManagedCisPolicy

`AmazonInspector2ManagedCisPolicy`adalah kebijakan AWS terkelola yang: Ini adalah kebijakan terkelola yang harus dilampirkan pelanggan pada peran mereka untuk berkomunikasi dengan layanan inspektur untuk pemindaian CIS

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonInspector2ManagedCisPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 Januari 2024, 16:31 UTC
- Waktu telah diedit: 24 Januari 2024, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonInspector2ReadOnlyAccess

`AmazonInspector2ReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya baca ke layanan inspektor2 Amazon dan layanan dukungan yang relevan

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonInspector2ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 21 Januari 2022, 14:45 UTC
- Waktu yang telah diedit: September 22, 2023, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "inspector2:BatchGet*",
        "inspector2:List*",
        "inspector2:Describe*",
        "inspector2:Get*",
        "inspector2:Search*",
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonInspector2ServiceRolePolicy

`AmazonInspector2ServiceRolePolicy`adalah kebijakan AWS terkelola yang: Memberikan akses kepada Amazon Inspector yang diperlukan Layanan AWS untuk melakukan penilaian keamanan

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 16 November 2021 20:27 UTC
- Waktu yang telah diedit: 22 Januari 2024, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TirosPolicy",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
```

```
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "tiros:CreateQuery",
        "tiros:GetQueryAnswer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PackageVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribeImages",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:ListImages",
        "ecr:PutRegistryScanningConfiguration",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "ssm:DescribeAssociation",
        "ssm:DescribeAssociationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:ListAssociations",
        "ssm:ListResourceDataSync"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaPackageVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions",
        "lambda:GetFunction",
        "lambda:GetLayerVersion",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GatherInventory",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:StartAssociationsOnce",
        "ssm:DeleteAssociation",
        "ssm:UpdateAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AmazonInspector2-*",
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "DataSyncCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateResourceDataSync",
        "ssm:DeleteResourceDataSync"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:resource-data-sync/InspectorResourceDataSync-do-not-delete"
      ]
    },
    {
      "Sid" : "ManagedRules",
```

```
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
      ]
    },
    {
      "Sid" : "LambdaCodeVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:GetAccountConfiguration",
        "codeguru-security:GetFindings",
        "codeguru-security:GetScan",
        "codeguru-security:ListFindings",
        "codeguru-security:BatchGetFindings",
        "codeguru-security:DeleteScansByCategory"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CodeGuruCodeVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListAttachedRolePolicies",
        "iam:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
```

```
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "codeguru-security.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "Ec2DeepInspection",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:GetParameters",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/inspector-aws/service/inspector-linux-application-
paths"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowManagementOfServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel"
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/inspector2/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "AllowListServiceLinkedChannels",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListServiceLinkedChannels"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToRunInvokeCisSpecificDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AmazonInspector2-InvokeInspectorSsmPluginCIS"
      ]
    },
    {
      "Sid" : "AllowToRunCisCommandsToSpecificResources",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToPutCloudwatchMetricData",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Inspector2"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonInspectorFullAccess

`AmazonInspectorFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Inspector.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonInspectorFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 07 Oktober 2015, 17:08 UTC
- Waktu yang telah diedit: 21 Desember 2017 14.53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorFullAccess`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector:*",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "sns:ListTopics",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "inspector.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/inspector.amazonaws.com/
AWSServiceRoleForAmazonInspector",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "inspector.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonInspectorReadOnlyAccess

`AmazonInspectorReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Amazon Inspector.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonInspectorReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 07 Oktober 2015, 17:08 UTC
- Waktu yang telah diedit: 01 Oktober 2019 15.17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "sns:ListTopics",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonInspectorServiceRolePolicy

`AmazonInspectorServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memberikan akses Amazon Inspector untukLayanan AWS diperlukan untuk melakukan penilaian keamanan

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. peran Anda.

detail kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 November 2017, 15:48 UTC
- Waktu yang telah diedit: 11 September 2020 17.12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeVirtualGateways",
```

```
        "directconnect:DescribeVirtualInterfaces",
        "directconnect:DescribeTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonKendraFullAccess

`AmazonKendraFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Kendra melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonKendraFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 Desember 2019, 16:15 UTC
- Waktu yang telah diedit: 03 Desember 2019 16.15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "kendra.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonKendra-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kendra:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonKendraReadOnlyAccess

`AmazonKendraReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Amazon Kendra melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonKendraReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 Desember 2019, 16:13 UTC
- Waktu yang telah diedit: 27 Mei 2021 07.01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kendra:Describe*",
        "kendra:List*",
        "kendra:Query",
        "kendra:GetQuerySuggestions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonKeyspacesFullAccess

`AmazonKeyspacesFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke Amazon Keyspaces

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKeyspacesFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 April 2020, 17:06 UTC
- Waktu telah diedit: 03 Oktober 2023, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "CassandraFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cassandra:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchAlarmsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
      "Condition" : {
```

```
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KeyspacesReplicationServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
replication.cassandra.amazonaws.com/AWSServiceRoleForKeyspacesReplication",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "replication.cassandra.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2VpcReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonKeyspacesReadOnlyAccess

`AmazonKeyspacesReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Amazon Keyspaces

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonKeyspacesReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 23 April 2020, 17:07 UTC
- Waktu yang telah diedit: 07 Juli 2022, 14.54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan kebijakan kebijakan kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
```

```
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonKeyspacesReadOnlyAccess_v2

`AmazonKeyspacesReadOnlyAccess_v2`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya baca ke Amazon Keyspaces dan layanan terkaitAWS.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonKeyspacesReadOnlyAccess_v2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 September 2023, 17:01 UTC
- Waktu yang telah diedit: September 12, 2023, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonKinesisAnalyticsFullAccess

`AmazonKinesisAnalyticsFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Kinesis Analytics melaluiAWS Management Console.

Menggunakan kebijakan

Anda dapat melampirkan`AmazonKinesisAnalyticsFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 21 September 2016, 19:01 UTC
- Waktu yang telah diedit: 21 September 2016 19.01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : "kinesisanalytics:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:CreateStream",
        "kinesis:DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLogEvents",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicyVersions",
        "iam:ListRoles"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/kinesis-analytics*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonKinesisAnalyticsReadOnly

`AmazonKinesisAnalyticsReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke Amazon Kinesis Analytics melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonKinesisAnalyticsReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 21 September 2016, 18:16 UTC
- Waktu yang telah diedit: 21 September 2016 06.16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisanalytics:Describe*",
        "kinesisanalytics:Get*",
        "kinesisanalytics:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "logs:GetLogEvents",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicyVersions",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonKinesisFirehoseFullAccess

`AmazonKinesisFirehoseFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke semua Amazon Kinesis Firehose Delivery Streams.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonKinesisFirehoseFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 07 Oktober 2015, 18:45 UTC
- Waktu yang telah diedit: 07 Oktober 2015 18.45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "firehose:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonKinesisFirehoseReadOnlyAccess

`AmazonKinesisFirehoseReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke semua Amazon Kinesis Firehose Delivery Streams.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonKinesisFirehoseReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 07 Oktober 2015, 18:43 UTC
- Waktu yang telah diedit: 07 Oktober 2015 18.43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "firehose:Describe*",
        "firehose:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonKinesisFullAccess

`AmazonKinesisFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke semua aliran melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonKinesisFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 08.40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kinesis:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonKinesisReadOnlyAccess

`AmazonKinesisReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke semua aliran melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonKinesisReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 08.40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:Get*",
        "kinesis:List*",
        "kinesis:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonKinesisVideoStreamsFullAccess

`AmazonKinesisVideoStreamsFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Kinesis Video Streams melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonKinesisVideoStreamsFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Desember 2017, 23:27 UTC
- Waktu yang telah diedit: 01 Desember 2017 08.27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kinesisvideo:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonKinesisVideoStreamsReadOnlyAccess

`AmazonKinesisVideoStreamsReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja keAWS Kinesis Video Streams melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonKinesisVideoStreamsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Desember 2017, 23:14 UTC
- Waktu yang telah diedit: 01 Desember 2017 08.14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:Describe*",
        "kinesisvideo:Get*",
        "kinesisvideo:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonLaunchWizard_Fullaccess

`AmazonLaunchWizard_Fullaccess`adalah kebijakanAWS terkelola yang: Akses penuh ke WisayaAWS Peluncuran dan layanan lain yang diperlukan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonLaunchWizard_Fullaccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Agustus 2020, 17:47 UTC
- Waktu yang telah diedit: 22 Februari 2023, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess`

Versi kebijakan

Versi kebijakan:v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:List*",
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets",
        "route53:GetChange",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:List*",
        "cloudwatch:Get*",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateVpc",
        "ec2:CreateKeyPair",
```

```
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AllocateHosts",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateVolume",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVolumeAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVolume",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteKeyPair",
        "ec2:DeleteNatGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachVolume",
        "ec2:DeleteSnapshot",
        "ec2:AssociateRouteTable",
        "ec2:AssociateVpcCidrBlock",
        "ec2:DeleteNetworkAcl",
```

```
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DetachNetworkInterface",
        "ec2:DisassociateAddress",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:GetLaunchTemplateData",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:GetConsoleOutput",
        "ec2:GetPasswordData",
        "ec2:ReleaseAddress",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:ModifyInstancePlacement",
        "ec2:DeletePlacementGroup",
        "ec2:CreatePlacementGroup",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "ds:AddIpRoutes",
        "ds:CreateComputer",
        "ds:CreateMicrosoftAD",
        "ds:DeleteDirectory",
        "servicecatalog:AssociateProductWithPortfolio",
        "cloudformation:GetTemplateSummary",
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:Get*",
        "cloudformation:ListStacks",
        "cloudformation:SignalResource",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/LaunchWizard*/*",
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam::*:role/service-role/AmazonLambdaRoleForLaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream",
        "logs:DescribeLog*",
        "logs:PutLogEvents",
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "sns:ListSubscriptionsByTopic",
        "sns:Publish",
        "ssm:DeleteDocument",
        "ssm:DeleteParameter*",
        "ssm:DescribeDocument*",
        "ssm:GetDocument",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/LaunchWizard*",
        "arn:aws:sns:*:*:*",
```

```
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*",
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunShellScript"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogStream",
        "logs:GetLogEvents",
        "logs:PutLogEvents",
        "ssm:AddTagsToResource",
        "ssm:DescribeDocument",
        "ssm:GetDocument",
```

```
        "ssm:ListTagsForResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "ds:Describe*",
        "ds:ListAuthorizedApplications",
        "ec2:Describe*",
        "ec2:Get*",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:List*",
        "logs:CreateLogGroup",
        "logs:GetLogDelivery",
        "logs:GetLogRecord",
        "logs:ListLogDeliveries",
        "resource-groups:Get*",
        "resource-groups:List*",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListServiceQuotas",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "ssm:CreateDocument",
        "ssm:DescribeAutomation*",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetCommandInvocation",
```

```
        "ssm:GetParameter*",
        "ssm:GetConnectionStatus",
        "ssm:ListCommand*",
        "ssm:ListDocument*",
        "ssm:ListInstanceAssociations",
        "ssm:SendAutomationSignal",
        "tag:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLog*",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:List*",
        "cloudformation:Describe*"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "application-insights.amazonaws.com",
            "events.amazonaws.com",
            "autoscaling.amazonaws.com.cn",
            "events.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "launchwizard:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
        "sqs:GetQueueUrl",
        "sqs:AddPermission",
        "sqs:ListQueues",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "iam:GetInstanceProfile",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "route53:ListHostedZones",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::launchwizard*/*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
```

```
        "s3:DeleteBucket",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:LaunchWizard*",
        "arn:aws:s3:::launchwizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DescribeTable",
        "dynamodb:DeleteTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsMetadata"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:DeleteOpsMetadata",
      "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:UntagResource",
        "fsx:TagResource",
        "fsx:DeleteFileSystem",
        "fsx:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/Name" : "LaunchWizard*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateFileSystem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:RequestTag/Name" : [
            "LaunchWizard*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:CreatePortfolio",
        "servicecatalog:DescribePortfolio",
        "servicecatalog:CreateConstraint",
        "servicecatalog:CreateProduct",
        "servicecatalog:AssociatePrincipalWithPortfolio",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:TagResource",
        "servicecatalog:UntagResource"
      ],
      "Resource" : [
        "arn:aws:servicecatalog:*:*:*/*",
        "arn:aws:catalog:*:*:*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:TagResource",
        "logs:UntagResource"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:LaunchWizard*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan ambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonLaunchWizardFullAccessV2

`AmazonLaunchWizardFullAccessV2`adalah sebuahAWSkebijakan terkelolaitu: Akses penuh keAWSLuncurkan wizard dan layanan lain yang diperlukan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonLaunchWizardFullAccessV2`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Tipe:AWSkebijakan terkelola
- Waktu pembuatan: 01 September 2023, 17:14 UTC
- Waktu yang diedit:01 September 2023, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2`

Versi kebijakan

Versi kebijakan: v1(default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber dayaAWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppInsightsActions0",
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupActions0",
```

```
      "Effect" : "Allow",
      "Action" : "resource-groups:List*",
      "Resource" : "*"
    },
    {
      "Sid" : "Route53Actions0",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets",
        "route53:GetChange",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3Actions0",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsActions0",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchActions0",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:List*",
        "cloudwatch:Get*",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "Ec2Actions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateVpc",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2Actions1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AllocateHosts",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateVolume",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVolumeAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVolume",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteKeyPair",
```

```
        "ec2:DeleteNatGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachVolume",
        "ec2:DeleteSnapshot",
        "ec2:AssociateRouteTable",
        "ec2:AssociateVpcCidrBlock",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DetachNetworkInterface",
        "ec2:DisassociateAddress",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:GetLaunchTemplateData",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:GetConsoleOutput",
        "ec2:GetPasswordData",
        "ec2:ReleaseAddress",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:ModifyInstancePlacement",
        "ec2:DeletePlacementGroup",
        "ec2:CreatePlacementGroup",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "ds:AddIpRoutes",
        "ds:CreateComputer",
        "ds:CreateMicrosoftAD",
        "ds:DeleteDirectory",
        "servicecatalog:AssociateProductWithPortfolio",
        "cloudformation:GetTemplateSummary",
        "sts:GetCallerIdentity"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormationActions0",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:Get*",
        "cloudformation:ListStacks",
        "cloudformation:SignalResource",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/LaunchWizard*/*",
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/*"
      ]
    },
    {
      "Sid" : "Ec2Actions2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Sid" : "IamActions0",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
```

```
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
    },
    {
      "Sid" : "IamActions1",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard",
        "arn:aws:iam::*:role/service-role/AmazonLambdaRoleForLaunchWizard",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "AutoScalingActions0",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "sns:ListSubscriptionsByTopic",
        "sns:Publish",
```

```
        "ssm:DeleteDocument",
        "ssm:DeleteParameter*",
        "ssm:DescribeDocument*",
        "ssm:GetDocument",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/LaunchWizard*",
        "arn:aws:sns:*:*:*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
      ]
    },
    {
      "Sid" : "SsmActions0",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunShellScript"
      ]
    },
    {
      "Sid" : "SsmActions1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
```

```
    {
      "Sid" : "SsmActions2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:DescribeDocument",
        "ssm:GetDocument",
        "ssm:ListTagsForResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
      ]
    },
    {
      "Sid" : "SsmActions3",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "ds:Describe*",
        "ds:ListAuthorizedApplications",
        "ec2:Describe*",
        "ec2:Get*",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:List*",
        "resource-groups:Get*",
        "resource-groups:List*",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListServiceQuotas",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "ssm:CreateDocument",
        "ssm:DescribeAutomation*",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters",
```

```
        "ssm:GetAutomationExecution",
        "ssm:GetCommandInvocation",
        "ssm:GetParameter*",
        "ssm:GetConnectionStatus",
        "ssm:ListCommand*",
        "ssm:ListDocument*",
        "ssm:ListInstanceAssociations",
        "ssm:SendAutomationSignal",
        "tag:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SsmActions4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormationActions1",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:List*",
        "cloudformation:Describe*"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
    },
    {
      "Sid" : "IamActions2",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "application-insights.amazonaws.com",
            "events.amazonaws.com",
            "autoscaling.amazonaws.com.cn",
            "events.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchWizardActions0",
      "Effect" : "Allow",
      "Action" : "launchwizard:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SqsActions0",
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
        "sqs:GetQueueUrl",
        "sqs:AddPermission",
        "sqs:ListQueues",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
    },
    {
      "Sid" : "CloudWatchActions1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "iam:GetInstanceProfile",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
```

```
      ]
    },
    {
      "Sid" : "EfsActions0",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "route53:ListHostedZones",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3Actions1",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::launchwizard*/*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Sid" : "CloudFormationActions2",
      "Effect" : "Allow",
      "Action" : "cloudformation:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    },
    {
      "Sid" : "LambdaActions0",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
        "s3:DeleteBucket",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:LaunchWizard*",
        "arn:aws:s3:::launchwizard*"
      ]
    },
    {
      "Sid" : "DynamodbActions0",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DescribeTable",
        "dynamodb:DeleteTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
    },
    {
      "Sid" : "SecretsManagerActions0",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
    },
    {
      "Sid" : "SecretsManagerActions1",
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SsmActions5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsMetadata"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SsmActions6",
      "Effect" : "Allow",
      "Action" : "ssm:DeleteOpsMetadata",
      "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
    },
    {
      "Sid" : "SnsActions0",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
    },
    {
      "Sid" : "FsxActions0",
      "Effect" : "Allow",
      "Action" : [
        "fsx:UntagResource",
        "fsx:TagResource",
        "fsx:DeleteFileSystem",
        "fsx:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/Name" : "LaunchWizard*"
```

```
        }
      }
    },
    {
      "Sid" : "FsxActions1",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateFileSystem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : [
            "LaunchWizard*"
          ]
        }
      }
    },
    {
      "Sid" : "FsxActions2",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceCatalogActions0",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:CreatePortfolio",
        "servicecatalog:DescribePortfolio",
        "servicecatalog:CreateConstraint",
        "servicecatalog:CreateProduct",
        "servicecatalog:AssociatePrincipalWithPortfolio",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:TagResource",
        "servicecatalog:UntagResource"
      ],
      "Resource" : [
        "arn:aws:servicecatalog:*:*:*/*",
        "arn:aws:catalog:*:*:*/*"
      ],
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmActions7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EfsActions1",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LogsActions0",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DescribeLogStreams",
        "logs:UntagResource",
```

```
        "logs:TagResource",
        "logs:CreateLogGroup",
        "logs:DeleteLogStream",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogDelivery",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
        "logs:ListLogDeliveries"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:LaunchWizard*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*:log-stream:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LogsActions1",
      "Effect" : "Allow",
      "Action" : "logs:DescribeLogGroups",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "FsxActions3",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        },
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "launchwizard.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FsxActions4",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "launchwizard.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FsxActions5",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "launchwizard.amazonaws.com"
          ]
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai denganAWSkebijakan terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLexChannelsAccess

`AmazonLexChannelsAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memungkinkan pelanggan untuk memanggil Lex runtime dari saluran

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup,

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 Januari 2021, 20:12 UTC
- Waktu yang telah diedit: 13 Januari 2021 20.12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lex:ListBots"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonLexFullAccess

`AmazonLexFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke Amazon Lex melalui AWS Management Console. Juga menyediakan akses untuk membuat Peran Tertaut Layanan Lex dan memberikan izin Lex untuk memanggil serangkaian fungsi Lambda terbatas.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonLexFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 April 2017, 23:20 UTC

- Waktu telah diedit: 07 Februari 2024, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexFullAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexFullAccessStatement1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "lex:*",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech",
        "kendra:ListIndices",
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "logs:DescribeLogGroups",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement2",
```

```
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonLex*",
      "Condition" : {
        "StringEquals" : {
          "lambda:Principal" : "lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement3",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement4",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lex.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement5",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "channels.lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement6",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement7",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "channels.lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement8",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement9",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ]
    },
    {
```

```
      "Sid" : "AmazonLexFullAccessStatement10",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lex.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement11",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lexv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement12",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "channels.lexv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement13",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lexv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLexReadOnly

`AmazonLexReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke Amazon Lex.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonLexReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 April 2017, 23:13 UTC
- Waktu yang telah diedit: 31 Januari 2023, 19.31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexReadOnly`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lex:GetBot",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "lex:GetBots",
        "lex:GetBotChannelAssociation",
        "lex:GetBotChannelAssociations",
        "lex:GetBotVersions",
        "lex:GetBuiltinIntent",
```

```
        "lex:GetBuiltinIntents",
        "lex:GetBuiltinSlotTypes",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetIntentVersions",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetSlotTypeVersions",
        "lex:GetUtterancesView",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotChannel",
        "lex:DescribeBotLocale",
        "lex:DescribeBotRecommendation",
        "lex:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
        "lex:ListBots",
        "lex:ListBotLocales",
        "lex:ListBotAliases",
        "lex:ListBotChannels",
        "lex:ListBotRecommendations",
        "lex:ListBotVersions",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
        "lex:ListImports",
        "lex:ListIntents",
        "lex:ListRecommendedIntents",
        "lex:ListSlots",
        "lex:ListSlotTypes",
        "lex:ListTagsForResource",
        "lex:SearchAssociatedTranscripts",
        "lex:ListCustomVocabularyItems"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonLexReplicationPolicy

`AmazonLexReplicationPolicy`adalah kebijakan AWS terkelola yang: Memungkinkan Amazon Lex mereplikasi sumber daya Lex di seluruh wilayah atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 31 Januari 2024, 23:29 UTC
- Waktu telah diedit: 08 Maret 2024, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "ReplicationServicePolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "lex:BuildBotLocale",
        "lex:ListBotLocales",
        "lex:CreateBotAlias",
        "lex:UpdateBotAlias",
        "lex:DeleteBotAlias",
        "lex:DescribeBotAlias",
        "lex:CreateBotVersion",
        "lex:DeleteBotVersion",
        "lex:DescribeBotVersion",
        "lex:CreateExport",
        "lex:DescribeBot",
        "lex:UpdateExport",
        "lex:DescribeExport",
        "lex:DescribeBotLocale",
        "lex:DescribeIntent",
        "lex:ListIntents",
        "lex:DescribeSlotType",
        "lex:ListSlotTypes",
        "lex:DescribeSlot",
        "lex:ListSlots",
        "lex:DescribeCustomVocabulary",
        "lex:StartImport",
        "lex:DescribeImport",
        "lex:CreateBot",
        "lex:UpdateBot",
        "lex:DeleteBot",
        "lex:CreateBotLocale",
        "lex:UpdateBotLocale",
        "lex:DeleteBotLocale",
        "lex:CreateIntent",
        "lex:UpdateIntent",
        "lex:DeleteIntent",
        "lex:CreateSlotType",
        "lex:UpdateSlotType",
        "lex:DeleteSlotType",
        "lex:CreateSlot",
        "lex:UpdateSlot",
        "lex:DeleteSlot",
        "lex:CreateCustomVocabulary",
```

```
        "lex:UpdateCustomVocabulary",
        "lex:DeleteCustomVocabulary",
        "lex:DeleteBotChannel",
        "lex:DeleteResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:lex:*:*:bot/*",
        "arn:aws:lex:*:*:bot-alias/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReplicationServicePolicyStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lex:CreateUploadUrl",
        "lex:ListBots"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReplicationServicePolicyStatement3",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lexv2.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonLexRunBotsOnly

`AmazonLexRunBotsOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses ke API percakapan Amazon Lex.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonLexRunBotsOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 April 2017, 23:06 UTC
- Waktu yang telah diedit: 18 Agustus 2021 09.15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexRunBotsOnly`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lex:PostContent",
        "lex:PostText",
        "lex:PutSession",
        "lex:GetSession",
        "lex:DeleteSession",
        "lex:RecognizeText",
        "lex:RecognizeUtterance",
        "lex:StartConversation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonLexV2BotPolicy

`AmazonLexV2BotPolicy`adalah kebijakan yangAWS dikelola yang: Menyediakan akses bot Lex V2 untuk memanggilAWS layanan lain atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan

- Waktu pembuatan: 13 Januari 2021, 20:10 UTC
- Waktu yang telah diedit: 13 Januari 2021 20.10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonLookoutEquipmentFullAccess

`AmazonLookoutEquipmentFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke operasi Amazon Lookout for Equipment

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonLookoutEquipmentFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 April 2021, 15:52 UTC
- Waktu yang telah diedit: 24 November 2021 21.00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutequipment:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : [
            "lookoutequipment.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "lookoutequipment.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus identitas identitas IAM IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonLookoutEquipmentReadOnlyAccess

`AmazonLookoutEquipmentReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Amazon Lookout for Equipments

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonLookoutEquipmentReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 05 Mei 2021, 16:47 UTC
- Waktu yang telah diedit: 10 November 2022, 22.04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutequipment:Describe*",
        "lookoutequipment:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonLookoutMetricsFullAccess

`AmazonLookoutMetricsFullAccess`adalah kebijakanAWS terkelola yang: Memberikan akses ke semua tindakan untuk Amazon Lookout for Metrics

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonLookoutMetricsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 07 Mei 2021, 00:43 UTC
- Waktu yang telah diedit: 07 Mei 2021 01.43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "lookoutmetrics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*LookoutMetrics*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lookoutmetrics.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonLookoutMetricsReadOnlyAccess

`AmazonLookoutMetricsReadOnlyAccess`adalah kebijakanAWS terkelola yang: Memberikan akses ke semua tindakan hanya-baca untuk Amazon Lookout for Metrics

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonLookoutMetricsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 07 Mei 2021, 00:43 UTC
- Waktu yang telah diedit: 04 Januari 2022, 18.19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutmetrics:DescribeMetricSet",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:DescribeAnomalyDetectionExecutions",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListTagsForResource",
        "lookoutmetrics:ListAnomalyGroupSummaries",
        "lookoutmetrics:ListAnomalyGroupTimeSeries",
        "lookoutmetrics:ListAnomalyGroupRelatedMetrics",
        "lookoutmetrics:GetAnomalyGroup",
        "lookoutmetrics:GetDataQualityMetrics",
        "lookoutmetrics:GetSampleData",
        "lookoutmetrics:GetFeedback"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonLookoutVisionConsoleFullAccess

`AmazonLookoutVisionConsoleFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Lookout for Vision dan akses scoped ke layanan yang diperlukan dan dependensi konsol.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonLookoutVisionConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Mei 2021, 19:37 UTC
- Waktu yang telah diedit: 11 Mei 2021 07.37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "LookoutVisionFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketSearchAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketFirstUseSetupAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketVersioning"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
```

```
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*/*"
    },
    {
      "Sid" : "LookoutVisionConsoleDatasetLabelingToolsAccess",
      "Effect" : "Allow",
      "Action" : [
        "groundtruthlabeling:RunGenerateManifestByCrawlingJob",
        "groundtruthlabeling:AssociatePatchToManifestJob",
        "groundtruthlabeling:DescribeConsoleJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleTagSelectorAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleKmsKeySelectorAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonLookoutVisionConsoleReadOnlyAccess

`AmazonLookoutVisionConsoleReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Amazon Lookout for Vision dan akses scoped ke layanan yang diperlukan dan dependensi konsol.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonLookoutVisionConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Mei 2021, 19:32 UTC
- Waktu yang telah diedit: 09 Desember 2021 02.46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeProject",
        "lookoutvision:DescribeTrialDetection",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "lookoutvision:ListTrialDetections",
        "lookoutvision:ListModelPackagingJobs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketSearchAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3ObjectReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*/*"
    },
    {
      "Sid" : "LookoutVisionConsoleDashboardAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonLookoutVisionFullAccess

`AmazonLookoutVisionFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Lookout for Vision dan akses scoped ke dependensi yang diperlukan.

Menggunakan kebijakan kebijakan kebijakan ini

Anda dapat melampirkan`AmazonLookoutVisionFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Mei 2021, 19:24 UTC
- Waktu yang telah diedit: 11 Mei 2021 07.24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi standar kebijakan kebijakan adalah versi yang menentukan izin kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonLookoutVisionReadOnlyAccess

`AmazonLookoutVisionReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Amazon Lookout for Vision dan akses cakupan ke dependensi yang diperlukan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonLookoutVisionReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Mei 2021, 19:11 UTC
- Waktu yang telah diedit: 09 Desember 2021 03.01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeProject",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "lookoutvision:ListModelPackagingJobs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan dan dan dan dan dan dan dan dan dan dan dan dan dan dan dan dan
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonMachineLearningBatchPredictionsAccess

`AmazonMachineLearningBatchPredictionsAccess`adalah kebijakanAWS terkelola yang: Memberikan izin kepada pengguna untuk meminta prediksi batch Amazon Machine Learning.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMachineLearningBatchPredictionsAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 April 2015, 17:12 UTC
- Waktu yang telah diedit: 09 April 2015 07.12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning:DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonMachineLearningCreateOnlyAccess

`AmazonMachineLearningCreateOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk sumber daya Amazon Machine Learning non-prediksi.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMachineLearningCreateOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 April 2015, 17:18 UTC
- Waktu yang telah diedit: 29 Juni 2016 20.55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning:Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonMachineLearningFullAccess

`AmazonMachineLearningFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke sumber daya Amazon Machine Learning.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMachineLearningFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 April 2015, 17:25 UTC
- Waktu yang telah diedit: 09 April 2015 07.25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

`AmazonMachineLearningManageRealTimeEndpointOnlyAccess`adalah kebijakanAWS terkelola yang: Memberikan izin kepada pengguna untuk membuat dan menghapus titik akhir waktu nyata untuk model Amazon Machine Learning.

Menggunakan kebijakan

Anda dapat melampirkan`AmazonMachineLearningManageRealTimeEndpointOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 April 2015, 17:32 UTC
- Waktu yang telah diedit: 09 April 2015 17.32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateRealtimeEndpoint",
        "machinelearning:DeleteRealtimeEndpoint"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonMachineLearningReadOnlyAccess

`AmazonMachineLearningReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke sumber daya Amazon Machine Learning.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMachineLearningReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 April 2015, 17:40 UTC
- Waktu yang telah diedit: 09 April 2015 07.40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonMachineLearningRealTimePredictionOnlyAccess

`AmazonMachineLearningRealTimePredictionOnlyAccess`adalah kebijakanAWS terkelola yang: Memberikan izin kepada pengguna untuk meminta prediksi waktu nyata Amazon Machine Learning.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMachineLearningRealTimePredictionOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 April 2015, 17:44 UTC
- Waktu yang telah diedit: 09 April 2015 17.44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Predict"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonMachineLearningRoleforRedshiftDataSourceV3

`AmazonMachineLearningRoleforRedshiftDataSourceV3`adalah kebijakanAWS terkelola yang: Memungkinkan Machine Learning mengonfigurasi dan menggunakan Kluster Redshift dan Lokasi Pementasan S3 untuk Sumber Data Redshift.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMachineLearningRoleforRedshiftDataSourceV3` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 24 Juni 2020, 18:00 UTC
- Waktu yang telah diedit: 24 Juni 2020, 18.00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan kebijakan kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupIngress",
        "redshift:AuthorizeClusterSecurityGroupIngress",
        "redshift:CreateClusterSecurityGroup",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:ModifyCluster",
        "redshift:RevokeClusterSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::amazon-machine-learning*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonMacieFullAccess

`AmazonMacieFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Macie.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMacieFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 14 Agustus 2017, 14:54 UTC
- Waktu yang telah diedit: 01 Juli 2022, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieFullAccess`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "pricing:GetProducts",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonMacieHandshakeRole

`AmazonMacieHandshakeRole`kebijakanAWS terkelola yang: Memberi izin untuk membuat peran tertaut layanan Amazon Macie.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMacieHandshakeRole` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 28 Juni 2018
- Waktu yang telah diedit: 28 Juni 2018 15.46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonMacieReadOnlyAccess

`AmazonMacieReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses readonly ke Amazon Macie.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMacieReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Juni 2023, 21:50 UTC

- Waktu yang diedit: 15 Juni 2023, 21.50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonMacieServiceRole

`AmazonMacieServiceRole`adalah kebijakanAWS terkelola di akun Anda untuk mengaktifkan analisis data

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMacieServiceRole` ke pengguna, grup, dan peran Anda.

detail kebijakan kebijakan terkelola ola

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Agustus 2017, 14:53 UTC
- Waktu yang telah diedit: 14 Agustus 2017 14.53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default untuk kebijakan yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON SON SON SON SON SON SON SON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonMacieServiceRolePolicy

`AmazonMacieServiceRolePolicy`adalah kebijakanAWS terkelola yang: Peran terkait layanan untuk Amazon Macie

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian detail kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 Juni 2018
- Waktu yang telah diedit: 19 Mei 2022, 19.16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccountAliases",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/macie/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonManagedBlockchainConsoleFullAccess

`AmazonManagedBlockchainConsoleFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Managed Blockchain melaluiAWS Management Console

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonManagedBlockchainConsoleFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 April 2019, 21:23 UTC
- Waktu yang telah diedit: 29 April 2019 09.23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonManagedBlockchainFullAccess

`AmazonManagedBlockchainFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Managed Blockchain.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonManagedBlockchainFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 April 2019, 21:39 UTC
- Waktu yang telah diedit: 29 April 2019 21.39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonManagedBlockchainReadOnlyAccess

`AmazonManagedBlockchainReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke Amazon Managed Blockchain.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonManagedBlockchainReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 April 2019, 18:17 UTC
- Waktu yang telah diedit: 30 April 2019 06.17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:Get*",
        "managedblockchain:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonManagedBlockchainServiceRolePolicy

`AmazonManagedBlockchainServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan akses keLayanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon Managed Blockchain

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup

Detail kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 Januari 2020

- Waktu yang telah diedit: 17 Januari 2020 19.51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/managedblockchain/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/managedblockchain/*:log-stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonMCSFullAccess

`AmazonMCSFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Managed Apache Cassandra Service

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMCSFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 Desember 2019, 13:45 UTC
- Waktu yang telah diedit: 17 April 2020, 19.19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
```

```
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonMCSReadOnlyAccess

`AmazonMCSReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Amazon Managed Apache Cassandra Service

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMCSReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 Desember 2019, 13:46 UTC
- Waktu yang telah diedit: 17 April 2020, 19.21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonMechanicalTurkFullAccess

`AmazonMechanicalTurkFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke semua API di Amazon Mechanical Turk.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMechanicalTurkFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Desember 2015, 19:08 UTC
- Waktu yang telah diedit: 11 Desember 2015 19.08 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mechanicalturk:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonMechanicalTurkReadOnly

`AmazonMechanicalTurkReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses ke API hanya baca di Amazon Mechanical Turk.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMechanicalTurkReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Desember 2015, 19:08 UTC
- Waktu yang telah diedit: 25 September 2019 21.06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mechanicalturk:Get*",
        "mechanicalturk:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus menghapus identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonMemoryDBFullAccess

`AmazonMemoryDBFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon MemoryDB melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMemoryDBFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 Oktober 2021, 19:24 UTC
- Waktu yang telah diedit: 08 Oktober 2021 19.24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : "memorydb:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/memorydb.amazonaws.com/
AWSServiceRoleForMemoryDB",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "memorydb.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonMemoryDBReadOnlyAccess

`AmazonMemoryDBReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Amazon MemoryDB melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMemoryDBReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 Oktober 2021, 19:27 UTC
- Waktu yang telah diedit: 08 Oktober 2021 19.27 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "memorydb:Describe*",
        "memorydb:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonMobileAnalyticsFinancialReportAccess

`AmazonMobileAnalyticsFinancialReportAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke semua laporan termasuk data keuangan untuk semua sumber daya aplikasi.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMobileAnalyticsFinancialReportAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 08.40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mobileanalytics:GetReports",
        "mobileanalytics:GetFinancialReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin izin identitas identitas identitas identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonMobileAnalyticsFullAccess

`AmazonMobileAnalyticsFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke semua sumber daya aplikasi.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMobileAnalyticsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 08.40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mobileanalytics:*",
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonMobileAnalyticsNon-financialReportAccess

`AmazonMobileAnalyticsNon-financialReportAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke laporan non keuangan untuk semua sumber daya aplikasi.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMobileAnalyticsNon-financialReportAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 08.40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mobileanalytics:GetReports",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonMobileAnalyticsWriteOnlyAccess

`AmazonMobileAnalyticsWriteOnlyAccess`adalah kebijakanAWS terkelola yang: Memberikan akses tulisnya saja agar dapat menempatkan data kejadian untuk semua sumber daya aplikasi. (Direkomendasikan untuk integrasi SDK)

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMobileAnalyticsWriteOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 08.40 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan ini adalah versi yang menentukan izin izin tulisnya. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mobileanalytics:PutEvents",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonMonitronFullAccess

`AmazonMonitronFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh untuk mengelola Amazon Monitron

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMonitronFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 02 Desember 2020, 22:40 UTC
- Waktu yang telah diedit: 08 Juni 2022, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMonitronFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "monitron.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "monitron:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "monitron.*.amazonaws.com"
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "AWSSSOPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "ds:DescribeDirectories",
        "ds:DescribeTrusts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
```

```
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/monitron/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonMQApiFullAccess

`AmazonMQApiFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke AmazonMQ melalui API/SDK kami.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMQApiFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 18 Desember 2018, 20:31 UTC
- Waktu yang telah diedit: 04 November 2020 16.45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mq:*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "iam:AWSServiceName" : "mq.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonMQApiReadOnlyAccess

`AmazonMQApiReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke AmazonMQ melalui API/SDK kami.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMQApiReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 18 Desember 2018 20:31 UTC
- Waktu yang telah diedit: 18 Desember 2018 20.31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonMQFullAccess

`AmazonMQFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke AmazonMQ melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMQFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 28 November 2017, 15:28 UTC
- Waktu yang telah diedit: 04 November 2020, 16.34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQFullAccess`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mq:*",
        "cloudformation:CreateStack",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "mq.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonMQReadOnlyAccess

`AmazonMQReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke AmazonMQ melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMQReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 28 November 2017, 15:30 UTC
- Waktu yang telah diedit: 28 November 2017 19.02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonMQServiceRolePolicy

`AmazonMQServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan Peran Tertaut Layanan untukAWS Amazon MQ

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 04 November 2020, 16:07 UTC
- Waktu yang telah diedit: 04 November 2020, 16.07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AMQManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:ResourceTag/AMQManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonMSKConnectReadOnlyAccess

`AmazonMSKConnectReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses readonly ke Amazon MSK Connect

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMSKConnectReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 20 September 2021, 10:18 UTC
- Waktu yang telah diedit: 18 Oktober 2021 09.16 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListWorkerConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeConnector"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:connector/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeCustomPlugin"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:custom-plugin/*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeWorkerConfiguration"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:worker-configuration/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonMSKFullAccess

`AmazonMSKFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke Amazon MSK dan izin lain yang diperlukan untuk dependensinya.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonMSKFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Januari 2019, 22:07 UTC
- Waktu telah diedit: 18 Oktober 2023, 11:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:*",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcAttribute",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "S3:GetBucketPolicy",
        "firehose:TagDeliveryStream"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*",
        "arn:*:ec2:*:*:subnet/*",
        "arn:*:ec2:*:*:security-group/*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "aws:RequestTag/ClusterArn" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "ec2:ResourceTag/ClusterArn" : "*"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "kafka.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/kafka.amazonaws.com/
AWSServiceRoleForKafka*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "kafka.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "delivery.logs.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonMSKReadOnlyAccess

`AmazonMSKReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses readonly ke Amazon MSK

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonMSKReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 14 Januari 2019, 22:28 UTC
- Waktu yang telah diedit: 14 Januari 2019 08.28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "kafka:Describe*",
        "kafka:List*",
        "kafka:Get*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcs",
        "kms:DescribeKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonMWAAServiceRolePolicy

`AmazonMWAAServiceRolePolicy`adalah kebijakanAWS terkelola yang: Peran Tertaut Layanan yang digunakan oleh Alur Kerja Terkelola Amazon untuk Apache Airflow.

Menggunakan kebijakan ini menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup

detail detail detail kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 November 2020, 14:13 UTC
- Waktu yang telah diedit: 17 November 2022, 00:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi standar kebijakan JSON adalah versi yang menentukan izin untuk kebijakan terampirkan ke versi default kebijakan terkelimpirkan ke versi yang menentukan izin untuk kebijakan terkelompokan kebijakan terkelimp Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:airflow-*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "AmazonMWAAManaged"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonMWAAManaged" : false
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "AmazonMWAAManaged"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/MWAA"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonNimbleStudio-LaunchProfileWorker

`AmazonNimbleStudio-LaunchProfileWorker`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan akses ke sumber daya yang dibutuhkan oleh pekerja Nimble Studio Launch Profile. Lampirkan kebijakan ini ke instans EC2 yang dibuat oleh Nimble Studio Builder.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonNimbleStudio-LaunchProfileWorker` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 28 April 2021, 04:47 UTC
- Waktu yang telah diedit: 28 April 2021 04.47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      },
      "Sid" : "GetLaunchProfileInitializationDependencies"
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonNimbleStudio-StudioAdmin

`AmazonNimbleStudio-StudioAdmin`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan akses ke sumber daya Amazon Nimble Studio yang terkait dengan admin studio dan sumber daya studio terkait di layanan lain. Lampirkan kebijakan ini ke peran Admin yang terkait dengan studio Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonNimbleStudio-StudioAdmin` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 April 2021, 04:47 UTC
- Waktu yang telah diedit: September 22, 2023, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Sid" : "StudioAdminFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "nimble:CreateStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
```

```
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:DeleteStreamingSession",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetEula",
        "nimble:AcceptEulas",
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListStreamingSessions",
        "nimble:GetStreamingImage",
        "nimble:ListStreamingImages",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents",
        "nimble:ListLaunchProfiles",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileMember",
        "nimble:ListLaunchProfileMembers",
        "nimble:PutLaunchProfileMembers",
        "nimble:UpdateLaunchProfileMember",
        "nimble:DeleteLaunchProfileMember"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
```

```
        "ds:DescribeDirectories",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      }
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonNimbleStudio-StudioUser

`AmazonNimbleStudio-StudioUser`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan akses ke sumber daya Amazon Nimble Studio yang terkait dengan pengguna studio dan sumber daya studio terkait di layanan lain. Lampirkan kebijakan ini ke peran Pengguna yang terkait dengan studio Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonNimbleStudio-StudioUser` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 April 2021, 04:48 UTC
- Waktu telah diedit: September 22, 2023, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource" : [
        "*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "nimble:ListLaunchProfiles"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "nimble:requesterPrincipalId" : "${nimble:principalId}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "nimble:DeleteStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:ListStreamingSessions",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "nimble:ownedBy" : "${nimble:requesterPrincipalId}"
        }
      }
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOmicsFullAccess

`AmazonOmicsFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Omics dan lainnya yang diperlukanLayanan AWS. Kebijakan ini memungkinkan pengguna untuk melihat dan menerima undangan berbagi RAM untuk mengakses sumber daya di luar penggunaAkun AWS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonOmicsFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Februari 2023, 00:59 UTC
- Waktu yang telah diedit: 24 Februari 2023, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "omics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "omics.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "omics.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonOmicsReadOnlyAccess

`AmazonOmicsReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Amazon Omics

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonOmicsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 November 2022, 04:17 UTC
- Waktu yang telah diedit: 29 November 2022, 04.17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "omics:Get*",
        "omics:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonOneEnterpriseFullAccess

`AmazonOneEnterpriseFullAccess`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin administratif yang memungkinkan akses ke semua sumber daya dan operasi Amazon One Enterprise.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOneEnterpriseFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2023, 04:58 UTC
- Waktu telah diedit: 28 November 2023, 04:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FullAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOneEnterpriseInstallerAccess

`AmazonOneEnterpriseInstallerAccess`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin baca dan tulis terbatas yang memungkinkan penginstalan dan aktivasi perangkat.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOneEnterpriseInstallerAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2023, 05:00 UTC
- Waktu telah diedit: 28 November 2023, 05:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
```

```
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOneEnterpriseReadOnlyAccess

`AmazonOneEnterpriseReadOnlyAccess`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin baca saja ke semua sumber daya dan operasi Amazon One Enterprise.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonOneEnterpriseReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2023, 04:59 UTC
- Waktu telah diedit: 28 November 2023, 04:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:Get*",
        "one:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOpenSearchDashboardsServiceRolePolicy

`AmazonOpenSearchDashboardsServiceRolePolicy`adalah kebijakan AWS terkelola yang: Menyediakan akses ke Layanan OpenSearch Dasbor Amazon untuk mengakses AWS layanan lain seperti CloudWatch atas nama Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 22 Desember 2023, 19:38 UTC
- Waktu telah diedit: 22 Desember 2023, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonOpenSearchDashboardsServiceRoleAllowedActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AOSD"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonOpenSearchIngestionFullAccess

`AmazonOpenSearchIngestionFullAccess`adalah kebijakanAWS terkelola yang: Memungkinkan AmazonOpenSearch Ingestion mengaksesAWS layanan lain atas nama Anda.

Menggunakan Kebijakan

Anda dapat melampirkan`AmazonOpenSearchIngestionFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 26 April 2023, 18:11 UTC
- Waktu yang telah diedit: 26 April 2023, 18.11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:CreatePipeline",
        "osis:UpdatePipeline",
        "osis:DeletePipeline",
        "osis:StartPipeline",
        "osis:StopPipeline",
        "osis:ListPipelines",
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:ValidatePipeline",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:TagResource",
        "osis:UntagResource",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/osis.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchIngestionService",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "osis.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonOpenSearchIngestionReadOnlyAccess

`AmazonOpenSearchIngestionReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke AmazonOpenSearch Ingestion Service

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonOpenSearchIngestionReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 26 April 2023, 18:09 UTC
- Waktu yang telah diedit: 26 April 2023, 18.09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan mengidentifikasi
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonOpenSearchIngestionServiceRolePolicy

`AmazonOpenSearchIngestionServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Amazon OpenSearch Ingestion Service mengaksesAWS layanan lain atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 November 2022, 16:49 UTC
- Waktu yang telah diedit: 18 November 2022, 16.49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OSISManaged" : "true"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OSISManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/OSIS"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonOpenSearchServerlessServiceRolePolicy

`AmazonOpenSearchServerlessServiceRolePolicy`adalah kebijakanAWS terkelola yang: Izinkan Amazon OpenSearch Tanpa Server mengaksesAWS layanan lain seperti CloudWatch API atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, grup, atau peran tidak dapat dilampirkan pada pengguna, grup, atau peran tidak dapat dilampirkan

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 November 2022, 19:50 UTC
- Waktu yang telah diedit: 24 November 2022, 19.50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan kebijakan ini. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AOSS"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonOpenSearchServiceCognitoAccess

`AmazonOpenSearchServiceCognitoAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses ke layanan konfigurasi Amazon Cognito.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonOpenSearchServiceCognitoAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 02 September 2021, 06:31 UTC
- Waktu yang telah diedit: 20 Desember 2021 14.04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:UpdateUserPoolClient",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:AdminInitiateAuth",
        "cognito-idp:AdminUserGlobalSignOut",
        "cognito-idp:ListUserPoolClients",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:UpdateIdentityPool",
        "cognito-identity:GetIdentityPoolRoles"
      ],
      "Resource" : [
        "arn:aws:cognito-identity:*:*:identitypool/*",
        "arn:aws:cognito-idp:*:*:userpool/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com",
            "cognito-identity-us-gov.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "cognito-identity:SetIdentityPoolRoles",
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonOpenSearchServiceFullAccess

`AmazonOpenSearchServiceFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke OpenSearch layanan konfigurasi Layanan Amazon.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonOpenSearchServiceFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 September 2021, 05:33 UTC
- Waktu yang telah diedit: 08 September 2021 05.33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonOpenSearchServiceReadOnlyAccess

`AmazonOpenSearchServiceReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke OpenSearch layanan konfigurasi Layanan Amazon.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonOpenSearchServiceReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 September 2021, 05:38 UTC
- Waktu yang telah diedit: 08 September 2021 05.38 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:Describe*",
        "es:List*",
        "es:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonOpenSearchServiceRolePolicy

`AmazonOpenSearchServiceRolePolicy`adalah kebijakan AWS terkelola yang: Izinkan Amazon OpenSearch Service mengakses AWS layanan lain seperti EC2 Networking API atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 Agustus 2021 09:27 UTC
- Waktu telah diedit: 23 Oktober 2023, 07:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
```

```
      "Sid" : "Stmt1480452973145",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973144",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973165",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973149",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973150",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
```

```
    {
      "Sid" : "Stmt1480452973154",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973164",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973174",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973184",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973194",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
```

```
    },
    {
      "Sid" : "Stmt1480452973195",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973196",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973197",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/ES"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973198",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973199",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973200",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973201",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973202",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonPersonalizeFullAccess

`AmazonPersonalizeFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Personalize melaluiAWS Management Console dan SDK. Juga menyediakan akses pilih ke layanan terkait (misalnya, S3, CloudWatch).

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonPersonalizeFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 04 Desember 2018, 22:24 UTC
- Waktu yang telah diedit: 30 Mei 2019 23.46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "personalize:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*Personalize*",
        "arn:aws:s3:::*personalize*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "personalize.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM yang menentukan izin
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonPollyFullAccess

`AmazonPollyFullAccess`adalah kebijakanAWS terkelola yang: Memberikan akses penuh ke layanan dan sumber daya Amazon Polly.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonPollyFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 November 2016, 18:59 UTC
- Waktu yang telah diedit: 30 November 2016 18.59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "polly:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonPollyReadOnlyAccess

`AmazonPollyReadOnlyAccess`adalah kebijakanAWS terkelola yang: Memberikan akses hanya-baca ke sumber daya Amazon Polly.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonPollyReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 November 2016, 18:59 UTC
- Waktu yang telah diedit: 17 Juli 2018 16.41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonPrometheusConsoleFullAccess

`AmazonPrometheusConsoleFullAccess`adalah kebijakanAWS terkelola yang: Memberikan akses penuh ke sumber daya PrometheusAWS Terkelola diAWS konsol

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonPrometheusConsoleFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 15 Desember 2020, 18:11 UTC
- Waktu yang telah diedit: 24 Oktober 2022, 22.25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagValues",
        "tag:GetTagKeys"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace",
        "aps:DescribeWorkspace",
        "aps:UpdateWorkspaceAlias",
```

```
        "aps:DeleteWorkspace",
        "aps:ListWorkspaces",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeRuleGroupsNamespace",
        "aps:CreateAlertManagerDefinition",
        "aps:CreateRuleGroupsNamespace",
        "aps:DeleteAlertManagerDefinition",
        "aps:DeleteRuleGroupsNamespace",
        "aps:ListRuleGroupsNamespaces",
        "aps:PutAlertManagerDefinition",
        "aps:PutRuleGroupsNamespace",
        "aps:TagResource",
        "aps:UntagResource",
        "aps:CreateLoggingConfiguration",
        "aps:UpdateLoggingConfiguration",
        "aps:DeleteLoggingConfiguration",
        "aps:DescribeLoggingConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonPrometheusFullAccess

`AmazonPrometheusFullAccess`adalah kebijakan AWS terkelola yang: Memberikan akses penuh ke sumber daya Prometheus AWS Terkelola

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonPrometheusFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Desember 2020, 18:10 UTC
- Waktu telah diedit: 26 November 2023, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllPrometheusActions",
      "Effect" : "Allow",
      "Action" : [
        "aps:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "aps.amazonaws.com"
```

```
          ]
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraper*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "scraper.aps.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonPrometheusQueryAccess

`AmazonPrometheusQueryAccess`adalah kebijakanAWS terkelola yang: Memberikan akses untuk menjalankan kueri terhadap sumber daya PrometheusAWS Terkelola

Menggunakan kebijakan

Anda dapat melampirkan`AmazonPrometheusQueryAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 19 Desember 2020, 01:02 UTC
- Waktu yang telah diedit: 19 Desember 2020, 01:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonPrometheusRemoteWriteAccess

`AmazonPrometheusRemoteWriteAccess`adalah kebijakanAWS terkelola yang: Hibah hanya menulis akses ke ruang kerja PrometheusAWS Terkelola

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonPrometheusRemoteWriteAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 19 Desember 2020, 01:04 UTC
- Waktu yang telah diedit: 19 Desember 2020, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:RemoteWrite"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonPrometheusScraperServiceRolePolicy

`AmazonPrometheusScraperServiceRolePolicy`adalah kebijakan AWS terkelola yang: Menyediakan akses ke AWS Sumber Daya yang dikelola atau digunakan oleh Amazon Managed Service untuk Prometheus Collector

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 November 2023, 14:19 UTC
- Waktu telah diedit: 26 November 2023, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScraperServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraper*"
    },
    {
      "Sid" : "NetworkDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ENIManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AMPAgentlessScraper"
          ]
        }
      }
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:*:ec2:*:*:network-interface/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "Null" : {
          "aws:RequestTag/AMPAgentlessScraper" : "false"
        }
      }
    },
    {
      "Sid" : "ENIUpdating",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AMPAgentlessScraper" : "false"
        }
      }
    },
    {
      "Sid" : "EKSAccess",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "arn:*:eks:*:*:cluster/*"
    },
    {
      "Sid" : "APSWriting",
      "Effect" : "Allow",
      "Action" : "aps:RemoteWrite",
      "Resource" : "arn:*:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonQFullAccess

`AmazonQFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh untuk mengaktifkan interaksi dengan Amazon Q

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonQFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2023, 16:00 UTC
- Waktu telah diedit: 28 November 2023, 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAmazonQFullAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "q:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonQLDBConsoleFullAccess

`AmazonQLDBConsoleFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon QLDB melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonQLDBConsoleFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 05 September 2019, 18:24 UTC
- Waktu yang telah diedit: 04 November 2022, 17.01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:CreateLedger",
        "qldb:UpdateLedger",
        "qldb:UpdateLedgerPermissionsMode",
        "qldb:DeleteLedger",
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ExportJournalToS3",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:CancelJournalKinesisStream",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:StreamJournalToKinesis",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:TagResource",
        "qldb:UntagResource",
        "qldb:ListTagsForResource",
        "qldb:SendCommand",
        "qldb:ExecuteStatement",
        "qldb:ShowCatalog",
        "qldb:InsertSampleData",
        "qldb:PartiQLCreateTable",
        "qldb:PartiQLCreateIndex",
        "qldb:PartiQLDropTable",
        "qldb:PartiQLDropIndex",
        "qldb:PartiQLUndropTable",
        "qldb:PartiQLDelete",
        "qldb:PartiQLInsert",
        "qldb:PartiQLUpdate",
        "qldb:PartiQLSelect",
        "qldb:PartiQLHistoryFunction",
        "qldb:PartiQLRedact"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dbqms:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:ListStreams",
        "kinesis:DescribeStream"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "qldb.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonQLDBFullAccess

`AmazonQLDBFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon QLDB melalui API layanan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonQLDBFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 05 September 2019, 18:23 UTC
- Waktu yang telah diedit: 04 November 2022, 17.01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBFullAccess`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:CreateLedger",
        "qldb:UpdateLedger",
        "qldb:UpdateLedgerPermissionsMode",
        "qldb:DeleteLedger",
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ExportJournalToS3",
        "qldb:ListJournalS3Exports",
```

```
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:CancelJournalKinesisStream",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:StreamJournalToKinesis",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:GetBlock",
        "qldb:TagResource",
        "qldb:UntagResource",
        "qldb:ListTagsForResource",
        "qldb:SendCommand",
        "qldb:PartiQLCreateTable",
        "qldb:PartiQLCreateIndex",
        "qldb:PartiQLDropTable",
        "qldb:PartiQLDropIndex",
        "qldb:PartiQLUndropTable",
        "qldb:PartiQLDelete",
        "qldb:PartiQLInsert",
        "qldb:PartiQLUpdate",
        "qldb:PartiQLSelect",
        "qldb:PartiQLHistoryFunction",
        "qldb:PartiQLRedact"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "qldb.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonQLDBReadOnly

`AmazonQLDBReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Amazon QLDB.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonQLDBReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 05 September 2019, 18:19 UTC
- Waktu yang telah diedit: 02 Juli 2021, 02.17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBReadOnly`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan kebijakan kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonRDSBetaServiceRolePolicy

`AmazonRDSBetaServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Amazon RDS mengelolaAWS sumber daya atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran baru.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 02 Mei 2018, 19:41 UTC
- Waktu yang telah diedit: 14 Desember 2022, 18.33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v8 (default)

Kebijakan ini adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
```

```
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB",
            "AWS/Neptune",
            "AWS/RDS",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds-beta-us-east-1!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-beta-us-
east-1"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-beta-us-east-1!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-beta-us-
east-1"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonRDSCustomInstanceProfileRolePolicy

`AmazonRDSCustomInstanceProfileRolePolicy`adalah kebijakan AWS terkelola yang: Mengizinkan Amazon RDS Custom melakukan berbagai tindakan otomatisasi dan tugas manajemen basis data melalui profil instans EC2.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSCustomInstanceProfileRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Februari 2024, 17:42 UTC
- Waktu telah diedit: 27 Februari 2024, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ssmAgentPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssmAgentPermission2",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:GetManifest",
        "ssm:PutConfigurePackageResult"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssmAgentPermission4",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:OpenControlChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission5",
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "createEc2SnapshotPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createEc2SnapshotPermission2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createEc2SnapshotPermission3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
```

```
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createTagForEc2SnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateSnapshot",
            "CreateSnapshots"
          ]
        }
      }
    },
    {
      "Sid" : "rdsCustomS3ObjectPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:putObject",
        "s3:getObject",
        "s3:getObjectVersion",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "rdsCustomS3BucketPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucketVersions",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "readSecretsFromCpPermission",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createSecretsOnDpPermission",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : [
```

```
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : "custom-oracle-rac"
        }
      }
    },
    {
      "Sid" : "publishCwMetricsPermission",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "rdscustom/rds-custom-sqlserver-agent",
            "RDSCustomForOracle/Agent"
          ]
        }
      }
    },
    {
      "Sid" : "putEventsToEventBusPermission",
      "Effect" : "Allow",
      "Action" : "events:PutEvents",
      "Resource" : "arn:aws:events:*:*:event-bus/default"
    },
    {
      "Sid" : "cwlUploadPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutRetentionPolicy",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:rds-custom-instance-*"
    },
    {
      "Sid" : "sendMessageToSqsQueuePermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : "custom-sqlserver"
        }
      }
    },
    {
      "Sid" : "managePrivateIpOnEniPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : "custom-oracle-rac"
        }
      }
    },
    {
      "Sid" : "kmsPermissionWithSecret",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:*:secret:do-
not-delete-rds-custom-*"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "kmsPermissionWithS3",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-rds-custom-
*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSCustomPreviewServiceRolePolicy

`AmazonRDSCustomPreviewServiceRolePolicy`adalah kebijakan AWSterkelola yang: Kebijakan Peran Layanan Pratinjau Kustom Amazon RDS

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 08 Oktober 2021 21:44 UTC
- Waktu telah diedit: September 20, 2023, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
```

```
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Sid" : "eccRunInstances3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "eccKeyPair2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface1",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
```

```
    },
    {
      "Sid" : "eccNetworkInterface3",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
```

```
          ],
          "ec2:CreateAction" : [
            "CreateKeyPair",
            "RunInstances",
            "CreateNetworkInterface",
            "CreateVolume",
            "CreateSnapshots",
            "CopySnapshot",
            "AllocateAddress"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
```

```
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume4snapshot1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot2",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "iam1",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
```

```
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWSRDSCustom*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw2",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
```

```
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb3",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
```

```
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds-preview.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb4",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:EnableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds-preview.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb5",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
```

```
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager2",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSCustomServiceRolePolicy

`AmazonRDSCustomServiceRolePolicy`adalah kebijakan AWS terkelola yang: Mengizinkan Amazon RDS Custom mengelola AWS sumber daya atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 08 Oktober 2021 21:39 UTC
- Waktu telah diedit: September 20, 2023, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
```

```
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Sid" : "eccRunInstances3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccKeyPair2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface1",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "eccNetworkInterface3",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
```

```
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateKeyPair",
            "RunInstances",
            "CreateNetworkInterface",
            "CreateVolume",
            "CreateSnapshot",
            "CreateSnapshots",
            "CopySnapshot",
            "AllocateAddress"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
```

```
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "eccVolume4snapshot1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot",
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
```

```
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot4",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ]
        }
      }
    },
    {
      "Sid" : "iam1",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : "arn:aws:iam::*:role/AWSRDSCustom*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw2",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
```

```
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
```

```
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb3",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "eb4",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:EnableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb5",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "secretmanager2",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "sqs1",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:TagQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ]
        }
      }
    },
    {
      "Sid" : "sqs2",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
```

```
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:DeleteQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ]
        }
      }
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSDataFullAccess

`AmazonRDSDataFullAccess`adalah kebijakanAWS terkelola yang: Memungkinkan akses penuh untuk menggunakan API data RDS, API penyimpanan rahasia untuk kredensi database RDS, dan API manajemen kueri konsol DB untuk mengeksekusi pernyataan SQL pada klaster Aurora Tanpa Server diAkun AWS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRDSDataFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 20 November 2018, 21:29 UTC
- Waktu yang telah diedit: 20 November 2019 09.58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSDataFullAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan kebijakan ini adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON JSON JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerDbCredentialsAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-db-credentials/*"
    },
    {
      "Sid" : "RDSDataServiceAccess",
      "Effect" : "Allow",
      "Action" : [
        "dbqms:CreateFavoriteQuery",
        "dbqms:DescribeFavoriteQueries",
        "dbqms:UpdateFavoriteQuery",
```

```
        "dbqms:DeleteFavoriteQueries",
        "dbqms:GetQueryString",
        "dbqms:CreateQueryHistory",
        "dbqms:DescribeQueryHistory",
        "dbqms:UpdateQueryHistory",
        "dbqms:DeleteQueryHistory",
        "rds-data:ExecuteSql",
        "rds-data:ExecuteStatement",
        "rds-data:BatchExecuteStatement",
        "rds-data:BeginTransaction",
        "rds-data:CommitTransaction",
        "rds-data:RollbackTransaction",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:GetRandomPassword",
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonRDSDirectoryServiceAccess

`AmazonRDSDirectoryServiceAccess`adalah kebijakanAWS terkelola yang: Izinkan RDS untuk mengakses Directory Service Managed AD atas nama pelanggan untuk contoh SQL Server DB yang bergabung dengan domain.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRDSDirectoryServiceAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Februari 2016, 02:02 UTC
- Waktu yang telah diedit: 15 Mei 2019 16.51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonRDSEnhancedMonitoringRole

`AmazonRDSEnhancedMonitoringRole`adalah kebijakanAWS terkelola yang: Menyediakan akses ke Cloudwatch untuk RDS Enhanced Monitoring

Menggunakan kebijakan

Anda dapat melampirkan`AmazonRDSEnhancedMonitoringRole` ke pengguna, grup, dan peran Anda.

Rincian

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 November 2015, 19:58 UTC
- Waktu yang telah diedit: 11 November 2015 19.58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EnableCreationAndManagementOfRDSCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
```

```
      "Resource" : [
        "arn:aws:logs:*:*:log-group:RDS*"
      ]
    },
    {
      "Sid" : "EnableCreationAndManagementOfRDSCloudwatchLogStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:RDS*:log-stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonRDSFullAccess

`AmazonRDSFullAccess`adalah sebuahAWSkebijakan terkelolaitu: Menyediakan akses penuh ke Amazon RDS melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRDSFullAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC

- Waktu yang diedit:17 Agustus 2023, 23:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSFullAccess`

Versi kebijakan

Versi kebijakan: v14(default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
```

```
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:GetCoipPoolUsage",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "outposts:GetOutpostInstanceTypes",
        "devops-guru:GetResourceCollection"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "pi:*",
      "Resource" : [
        "arn:aws:pi:*:*:metrics/rds/*",
        "arn:aws:pi:*:*:perf-reports/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "rds.amazonaws.com",
            "rds.application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "devops-guru:SearchInsights",
        "devops-guru:ListAnomaliesForInsight"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "devops-guru:ServiceNames" : [
            "RDS"
          ]
        },
        "Null" : {
          "devops-guru:ServiceNames" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai denganAWSkebijakan terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSPerformanceInsightsFullAccess

`AmazonRDSPerformanceInsightsFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke RDS Performance Insights melalui AWS Management Console

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSPerformanceInsightsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Agustus 2023, 23:41 UTC
- Waktu yang telah diedit: 23 Oktober 2023, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSPerformanceInsightsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics"
      ],
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsAnalisysReportFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:CreatePerformanceAnalysisReport",
        "pi:GetPerformanceAnalysisReport",
        "pi:ListPerformanceAnalysisReports",
        "pi:DeletePerformanceAnalysisReport"
      ],
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsTaggingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:TagResource",
        "pi:UntagResource",
```

```
        "pi:ListTagsForResource"
      ],
      "Resource" : "arn:aws:pi:*:*:*/rds/*"
    },
    {
      "Sid" : "AmazonRDSDescribeInstanceAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCloudWatchReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSPerformanceInsightsReadOnly

`AmazonRDSPerformanceInsightsReadOnly`adalah kebijakan AWS terkelola yang: Kebijakan Read-Only untuk RDS Performance Insights

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRDSPerformanceInsightsReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 April 2022, 00:02 UTC
- Waktu yang telah diedit: 23 Oktober 2023, 21:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSDescribeDBInstances",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRDSDescribeDBClusters",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBClusters",
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsDescribeDimensionKeys",
      "Effect" : "Allow",
```

```
      "Action" : "pi:DescribeDimensionKeys",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetDimensionKeyDetails",
      "Effect" : "Allow",
      "Action" : "pi:GetDimensionKeyDetails",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetadata",
      "Effect" : "Allow",
      "Action" : "pi:GetResourceMetadata",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetrics",
      "Effect" : "Allow",
      "Action" : "pi:GetResourceMetrics",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceDimensions",
      "Effect" : "Allow",
      "Action" : "pi:ListAvailableResourceDimensions",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceMetrics",
      "Effect" : "Allow",
      "Action" : "pi:ListAvailableResourceMetrics",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetPerformanceAnalysisReport",
      "Effect" : "Allow",
      "Action" : "pi:GetPerformanceAnalysisReport",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListPerformanceAnalysisReports",
      "Effect" : "Allow",
      "Action" : "pi:ListPerformanceAnalysisReports",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
```

```
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListTagsForResource",
      "Effect" : "Allow",
      "Action" : "pi:ListTagsForResource",
      "Resource" : "arn:aws:pi:*:*:*/rds/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSPreviewServiceRolePolicy

`AmazonRDSPreviewServiceRolePolicy`adalah kebijakan AWSterkelola yang: Kebijakan Peran Layanan Pratinjau Amazon RDS

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 31 Mei 2018, 18:02 UTC
- Waktu telah diedit: 04 Oktober 2023, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB-Preview",
            "AWS/Neptune-Preview",
            "AWS/RDS-Preview",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds-preview-us-east-2!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-preview-
us-east-2"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-preview-us-east-2!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-preview-
us-east-2"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRDSReadOnlyAccess

`AmazonRDSReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Amazon RDS melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRDSReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 14 April 2023, 12.32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:Describe*",
        "rds:ListTagsForResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "devops-guru:GetResourceCollection"
      ],
      "Resource" : "*"
    },
    {
      "Action" : [
        "devops-guru:SearchInsights",
        "devops-guru:ListAnomaliesForInsight"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "devops-guru:ServiceNames" : [
            "RDS"
          ]
        },
        "Null" : {
          "devops-guru:ServiceNames" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonRDSServiceRolePolicy

`AmazonRDSServiceRolePolicy`adalah kebijakan AWS terkelola yang: Memungkinkan Amazon RDS mengelola AWS sumber daya atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 08 Januari 2018, 18:17 UTC
- Waktu telah diedit: 19 Januari 2024, 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CrossRegionCommunication",
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
```

```
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Sns",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*"
      ]
    },
    {
      "Sid" : "CloudWatchStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
```

```
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    },
    {
      "Sid" : "Kinesis",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:CreateStream",
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream",
        "kinesis:SplitShard",
        "kinesis:MergeShards",
        "kinesis:DeleteStream",
        "kinesis:UpdateShardCount"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/aws-rds-das-*"
      ]
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB",
            "AWS/Neptune",
            "AWS/RDS",
            "AWS/Usage"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "SecretsManagerPassword",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds"
        }
      }
    },
    {
      "Sid" : "SecretsManagerTags",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRedshiftAllCommandsFullAccess

`AmazonRedshiftAllCommandsFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini mencakup izin untuk menjalankan perintah SQL untuk menyalin, memuat, membongkar, membuat kueri, dan menganalisis data di Amazon Redshift. Kebijakan ini juga memberikan izin untuk menjalankan pernyataan terpilih untuk layanan terkait, seperti Amazon S3, CloudWatch log Amazon, Amazon SageMaker, atauAWS Glue.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRedshiftAllCommandsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 04 November 2021, 00:48 UTC
- Waktu yang telah diedit: 25 November 2021, 02.27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:InvokeEndpoint",
        "sagemaker:StopProcessingJob",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*redshift*",
        "arn:aws:sagemaker:*:*:training-job/*redshift*",
        "arn:aws:sagemaker:*:*:automl-job/*redshift*",
        "arn:aws:sagemaker:*:*:compilation-job/*redshift*",
        "arn:aws:sagemaker:*:*:processing-job/*redshift*",
        "arn:aws:sagemaker:*:*:transform-job/*redshift*",
        "arn:aws:sagemaker:*:*:endpoint/*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
```

```
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Endpoints/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/ProcessingJobs/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/TrainingJobs/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/TransformJobs/*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "SageMaker",
            "/aws/sagemaker/Endpoints",
            "/aws/sagemaker/ProcessingJobs",
            "/aws/sagemaker/TrainingJobs",
            "/aws/sagemaker/TransformJobs"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetEncryptionConfiguration",
```

```
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketCors",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::redshift-downloads",
        "arn:aws:s3:::redshift-downloads/*",
        "arn:aws:s3:::*redshift*",
        "arn:aws:s3:::*redshift*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/Redshift" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan",
        "dynamodb:DescribeTable",
        "dynamodb:Getitem"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/*redshift*",
        "arn:aws:dynamodb:*:*:table/*redshift*/index/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:ListInstances"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:ListInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "elasticmapreduce:ResourceTag/Redshift" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:*redshift*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
```

```
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*redshift*/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "redshift.amazonaws.com",
            "glue.amazonaws.com",
            "sagemaker.amazonaws.com",
```

```
            "athena.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonRedshiftDataFullAccess

`AmazonRedshiftDataFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini menyediakan akses penuh ke Amazon Redshift Data API. Kebijakan ini juga memberikan akses lingkup ke layanan lain yang diperlukan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRedshiftDataFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 September 2020, 19:23 UTC
- Waktu yang telah diedit: 07 April 2023, 18.18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/RedshiftDataFullAccess" : "*"
        }
      }
    },
    {
      "Sid" : "GetCredentialsForAPIUser",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
```

```
      "Resource" : [
        "arn:aws:redshift:*:*:dbname:*/*",
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Sid" : "GetCredentialsWithFederatedIAMCredentials",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentialsWithIAM",
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*"
    },
    {
      "Sid" : "GetCredentialsForServerless",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetCredentials",
      "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/RedshiftDataFullAccess" : "*"
        }
      }
    },
    {
      "Sid" : "DenyCreateAPIUser",
      "Effect" : "Deny",
      "Action" : "redshift:CreateClusterUser",
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Sid" : "ServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/redshift-data.amazonaws.com/
AWSServiceRoleForRedshift",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "redshift-data.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonRedshiftFullAccess

`AmazonRedshiftFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Redshift melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRedshiftFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 07 Juli 2022, 23.31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Action" : [
        "redshift:*",
        "redshift-serverless:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "sns:CreateTopic",
        "sns:Get*",
        "sns:List*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DisableAlarmActions",
        "tag:GetResources",
        "tag:UntagResources",
        "tag:GetTagValues",
        "tag:GetTagKeys",
        "tag:TagResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "redshift.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataAPIPermissions",
      "Action" : [
```

```
        "redshift-data:ExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerListPermissions",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerCreateGetPermissions",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/RedshiftDataFullAccess" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonRedshiftQueryEditor

`AmazonRedshiftQueryEditor`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Redshift Query Editor dan untuk kueri yang disimpan melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRedshiftQueryEditor` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 04 Oktober 2018, 22:50 UTC
- Waktu yang telah diedit: 16 Februari 2021 19.33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials",
```

```
        "redshift:ListSchemas",
        "redshift:ListTables",
        "redshift:ListDatabases",
        "redshift:ExecuteQuery",
        "redshift:FetchResults",
        "redshift:CancelQuery",
        "redshift:DescribeClusters",
        "redshift:DescribeQuery",
        "redshift:DescribeTable",
        "redshift:ViewQueriesFromConsole",
        "redshift:DescribeSavedQueries",
        "redshift:CreateSavedQuery",
        "redshift:DeleteSavedQueries",
        "redshift:ModifySavedQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataAPIPermissions",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "DataAPIIAMSessionPermissionsRestriction",
      "Action" : [
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:ListStatements"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
```

```
    },
    {
      "Sid" : "SecretsManagerListPermissions",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerCreateGetPermissions",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/RedshiftQueryOwner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonRedshiftQueryEditorV2FullAccess

`AmazonRedshiftQueryEditorV2FullAccess`adalah kebijakan AWS terkelola yang: Memberikan akses penuh ke operasi dan sumber daya Amazon Redshift Query Editor V2. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan. Ini termasuk izin untuk mencantumkan kluster

Amazon Redshift, kunci baca, dan alias AWS di KMS dan mengelola rahasia Query Editor V2 di Secrets Manager. AWS

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftQueryEditorV2FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 September 2021 14:06 UTC
- Waktu telah diedit: 21 Februari 2024, 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KeyManagementServicePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*"
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2Permissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRedshiftQueryEditorV2NoSharing

`AmazonRedshiftQueryEditorV2NoSharing`adalah kebijakan AWS terkelola yang: Memberikan kemampuan untuk bekerja dengan Amazon Redshift Query Editor V2 tanpa berbagi sumber daya. Prinsipal yang diberikan hanya dapat membaca, memperbarui, dan menghapus sumber dayanya sendiri tetapi tidak dapat membagikannya. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan. Ini termasuk izin untuk mencantumkan kluster Amazon Redshift dan mengelola rahasia Query Editor V2 dari prinsipal di Secrets Manager. AWS

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftQueryEditorV2NoSharing` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 September 2021 14:18 UTC
- Waktu telah diedit: 21 Februari 2024, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
```

```
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
```

```
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRedshiftQueryEditorV2ReadSharing

`AmazonRedshiftQueryEditorV2ReadSharing`adalah kebijakan AWS terkelola yang: Memberikan kemampuan untuk bekerja dengan Amazon Redshift Query Editor V2 dengan pembagian sumber daya yang terbatas. Kepala sekolah yang diberikan dapat membaca, menulis, dan berbagi sumber dayanya sendiri. Prinsipal yang diberikan dapat membaca sumber daya yang dibagikan dengan timnya tetapi tidak dapat memperbaruinya. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan. Ini termasuk izin untuk mencantumkan kluster Amazon Redshift dan mengelola rahasia Query Editor V2 dari prinsipal di Secrets Manager. AWS

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftQueryEditorV2ReadSharing` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 September 2021 14:22 UTC
- Waktu telah diedit: 21 Februari 2024, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
```

```
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
```

```
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
```

```
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
```

```
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TeamReadAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
```

```
      "Effect" : "Allow",
      "Action" : "sqlworkbench:UntagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRedshiftQueryEditorV2ReadWriteSharing

`AmazonRedshiftQueryEditorV2ReadWriteSharing`adalah kebijakan AWS terkelola yang: Memberikan kemampuan untuk bekerja dengan Amazon Redshift Query Editor V2 dengan berbagi sumber daya. Kepala sekolah yang diberikan dapat membaca, menulis, dan berbagi sumber dayanya sendiri. Kepala sekolah yang diberikan dapat membaca dan memperbarui sumber daya yang dibagikan dengan timnya. Kebijakan ini juga memberikan akses ke layanan lain yang diperlukan. Ini termasuk izin untuk mencantumkan kluster Amazon Redshift dan mengelola rahasia Query Editor V2 dari prinsipal di Secrets Manager. AWS

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftQueryEditorV2ReadWriteSharing` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 24 September 2021 14:25 UTC
- Waktu telah diedit: 21 Februari 2024, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
```

```
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
```

```
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
```

```
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TeamReadWriteAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
```

```
      "Effect" : "Allow",
      "Action" : "sqlworkbench:UntagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRedshiftReadOnlyAccess

`AmazonRedshiftReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya baca ke Amazon Redshift melalui. AWS Management Console

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRedshiftReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 08 Februari 2024, 00:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRedshiftReadOnlyAccess",
      "Action" : [
        "redshift:Describe*",
        "redshift:ListRecommendations",
        "redshift:ViewQueriesInConsole",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "sns:Get*",
        "sns:List*",
        "cloudwatch:Describe*",
        "cloudwatch:List*",
        "cloudwatch:Get*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRedshiftServiceLinkedRolePolicy

`AmazonRedshiftServiceLinkedRolePolicy`adalah kebijakan AWS terkelola yang: Mengizinkan Amazon Redshift memanggil AWS layanan atas nama Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 September 2017, 19:19 UTC
- Waktu yang telah diedit: 15 Maret 2024, 20:00 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2VpcPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PublicAccessCreateEip",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "PublicAccessReleaseEip",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Redshift" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/redshift/*"
      ]
    },
    {
      "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/redshift/*:log-stream:*"
      ]
    },
    {
      "Sid" : "CreateSecurityGroupWithTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:ModifySecurityGroupRules",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateTagsOnResources",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpc",
```

```
            "CreateSecurityGroup",
            "CreateSubnet",
            "CreateInternetGateway",
            "CreateRouteTable",
            "AllocateAddress"
          ]
        }
      }
    },
    {
      "Sid" : "VPCPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Redshift-Serverless",
            "AWS/Redshift"
          ]
        }
      }
    },
    {
      "Sid" : "SecretManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
```

```
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:RotateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:redshift!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "redshift",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerRandomPassword",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IPV6Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "ServiceQuotasToCheckCustomerLimits",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:ec2/L-0263D0A3",
        "arn:aws:servicequotas:*:*:vpc/L-29B6F2EB"
```

```
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRekognitionCustomLabelsFullAccess

`AmazonRekognitionCustomLabelsFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini menetapkan izin rekognition dan s3 yang diperlukan oleh fitur Label Kustom Amazon Rekognition.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRekognitionCustomLabelsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 Januari 2020, 19:18 UTC
- Waktu yang telah diedit: 16 Agustus 2022, 20.20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*custom-labels*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rekognition:CreateProject",
        "rekognition:CreateProjectVersion",
        "rekognition:StartProjectVersion",
        "rekognition:StopProjectVersion",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DetectCustomLabels",
        "rekognition:DeleteProject",
        "rekognition:DeleteProjectVersion",
        "rekognition:TagResource",
        "rekognition:UntagResource",
        "rekognition:ListTagsForResource",
        "rekognition:CreateDataset",
        "rekognition:ListDatasetEntries",
        "rekognition:ListDatasetLabels",
        "rekognition:DescribeDataset",
        "rekognition:UpdateDatasetEntries",
        "rekognition:DistributeDatasetEntries",
        "rekognition:DeleteDataset",
        "rekognition:CopyProjectVersion",
        "rekognition:PutProjectPolicy",
        "rekognition:ListProjectPolicies",
        "rekognition:DeleteProjectPolicy"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonRekognitionFullAccess

`AmazonRekognitionFullAccess`adalah kebijakanAWS terkelola yang: Akses ke semua API Amazon Rekognition

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRekognitionFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 November 2016, 14:40 UTC
- Waktu yang telah diedit: 30 November 2016 14.40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rekognition:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonRekognitionReadOnlyAccess

`AmazonRekognitionReadOnlyAccess`adalah kebijakan AWS terkelola yang: Akses ke semua API Rekognition Baca

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRekognitionReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2016, 14:58 UTC
- Waktu telah diedit: November 08, 2023, 18:30 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRekognitionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "rekognition:CompareFaces",
        "rekognition:DetectFaces",
        "rekognition:DetectLabels",
        "rekognition:ListCollections",
        "rekognition:ListFaces",
        "rekognition:SearchFaces",
        "rekognition:SearchFacesByImage",
        "rekognition:DetectText",
        "rekognition:GetCelebrityInfo",
        "rekognition:RecognizeCelebrities",
        "rekognition:DetectModerationLabels",
        "rekognition:GetLabelDetection",
        "rekognition:GetFaceDetection",
        "rekognition:GetContentModeration",
        "rekognition:GetPersonTracking",
        "rekognition:GetCelebrityRecognition",
        "rekognition:GetFaceSearch",
        "rekognition:GetTextDetection",
        "rekognition:GetSegmentDetection",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListStreamProcessors",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
```

```
        "rekognition:DetectCustomLabels",
        "rekognition:DetectProtectiveEquipment",
        "rekognition:ListTagsForResource",
        "rekognition:ListDatasetEntries",
        "rekognition:ListDatasetLabels",
        "rekognition:DescribeDataset",
        "rekognition:ListProjectPolicies",
        "rekognition:ListUsers",
        "rekognition:SearchUsers",
        "rekognition:SearchUsersByImage",
        "rekognition:GetMediaAnalysisJob",
        "rekognition:ListMediaAnalysisJobs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRekognitionServiceRole

`AmazonRekognitionServiceRole`adalah kebijakanAWS terkelola yang: Memungkinkan Rekognition untuk memanggilAWS layanan atas nama Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRekognitionServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 29 November 2017

- Waktu yang telah diedit: 29 November 2017 16.52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:AmazonRekognition*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/AmazonRekognition*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:GetMedia"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonRoute53AutoNamingFullAccess

`AmazonRoute53AutoNamingFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke semua tindakan Penamaan Otomatis Route 53.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRoute53AutoNamingFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 18 Januari 2018, 18:40 UTC
- Waktu yang telah diedit: 18 Januari 2018 08.40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "servicediscovery:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonRoute53AutoNamingReadOnlyAccess

`AmazonRoute53AutoNamingReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke semua tindakan Penamaan Otomatis Route 53.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRoute53AutoNamingReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 18 Januari 2018, 03:02 UTC
- Waktu yang telah diedit: 18 Januari 2018 03.02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:Get*",
        "servicediscovery:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonRoute53AutoNamingRegistrantAccess

`AmazonRoute53AutoNamingRegistrantAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses tingkat pendaftar ke tindakan Penamaan Otomatis Route 53.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRoute53AutoNamingRegistrantAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 12 Maret 2018, 22:33 UTC
- Waktu yang telah diedit: 12 Maret 2018 02.33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
```

```
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:DeregisterInstance"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonRoute53DomainsFullAccess

`AmazonRoute53DomainsFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke semua tindakan Route53 Domain dan Buat Zona Hosted untuk memungkinkan pembuatan Zona Hosted sebagai bagian dari pendaftaran domain.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRoute53DomainsFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 08.40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonRoute53DomainsReadOnlyAccess

`AmazonRoute53DomainsReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses ke daftar dan tindakan Route53 Domain.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRoute53DomainsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 08.40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonRoute53FullAccess

`AmazonRoute53FullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke semua Amazon Route 53 melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRoute53FullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 20 Desember 2018 09.42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53FullAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:*",
        "route53domains:*",
        "cloudfront:ListDistributions",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticbeanstalk:DescribeEnvironments",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRegions",
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : "arn:aws:apigateway:*::/domainnames"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonRoute53ReadOnlyAccess

`AmazonRoute53ReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke semua Amazon Route 53 melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRoute53ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 15 November 2016 09.15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonRoute53RecoveryClusterFullAccess

`AmazonRoute53RecoveryClusterFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Cluster Pemulihan Amazon Route 53

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRoute53RecoveryClusterFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 18 Agustus 2021, 18:37 UTC
- Waktu yang telah diedit: 18 Agustus 2021 18.37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonRoute53RecoveryClusterReadOnlyAccess

`AmazonRoute53RecoveryClusterReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Cluster Pemulihan Amazon Route 53

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRoute53RecoveryClusterReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 18 Agustus 2021, 17:36 UTC
- Waktu yang telah diedit: 01 April 2022, 17.37 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonRoute53RecoveryControlConfigFullAccess

`AmazonRoute53RecoveryControlConfigFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Route 53 Recovery Control Config

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRoute53RecoveryControlConfigFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 18 Agustus 2021, 17:48 UTC
- Waktu yang telah diedit: 18 Agustus 2021 17.48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonRoute53RecoveryControlConfigReadOnlyAccess

`AmazonRoute53RecoveryControlConfigReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses baca saja ke Amazon Route 53 Recovery Control Config

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonRoute53RecoveryControlConfigReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Agustus 2021, 18:01 UTC
- Waktu yang telah diedit: 18 Oktober 2023, 17:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeRoutingControlByName",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:ListAssociatedRoute53HealthChecks",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonRoute53RecoveryReadinessFullAccess

`AmazonRoute53RecoveryReadinessFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Kesiapan Pemulihan Amazon Route 53

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRoute53RecoveryReadinessFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 18 Agustus 2021, 16:45 UTC

- Waktu yang telah diedit: 18 Agustus 2021 16.45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonRoute53RecoveryReadinessReadOnlyAccess

`AmazonRoute53RecoveryReadinessReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Kesiapan Pemulihan Amazon Route 53

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRoute53RecoveryReadinessReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 18 Agustus 2021, 18:11 UTC
- Waktu yang telah diedit: 09 November 2021 20.14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetReadinessCheckResourceStatus",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListCrossAccountAuthorizations",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
```

```
        "route53-recovery-readiness:ListRules",
        "route53-recovery-readiness:ListTagsForResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetArchitectureRecommendations",
        "route53-recovery-readiness:GetCellReadinessSummary"
      ],
      "Resource" : "arn:aws:route53-recovery-readiness::*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonRoute53ResolverFullAccess

`AmazonRoute53ResolverFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan akses penuh untuk Route 53 Resolver

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRoute53ResolverFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 Mei 2019, 18:10 UTC
- Waktu yang telah diedit: 17 Juli 2020, 19.03 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:*",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonRoute53ResolverReadOnlyAccess

`AmazonRoute53ResolverReadOnlyAccess`adalah kebijakanAWS terkelola yang: Kebijakan baca saja untuk Route 53 Resolver

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonRoute53ResolverReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 Mei 2019, 18:11 UTC
- Waktu yang telah diedit: 27 September 2019 16.37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonS3FullAccess

`AmazonS3FullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke semua bucket melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonS3FullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 27 September 2021 20.16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:*",
        "s3-object-lambda:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonS3ObjectLambdaExecutionRolePolicy

`AmazonS3ObjectLambdaExecutionRolePolicy`adalah kebijakanAWS terkelola yang: Menyediakan izin fungsiAWS Lambda untuk berinteraksi dengan Amazon S3 Object Lambda. Juga memberikan izin Lambda untuk menulis ke CloudWatch Log.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonS3ObjectLambdaExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 18 Agustus 2021, 10:07 UTC
- Waktu yang telah diedit: 18 Agustus 2021 10.07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonS3OutpostsFullAccess

`AmazonS3OutpostsFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon S3 di Outposts melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonS3OutpostsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 02 Oktober 2020, 17:26 UTC
- Waktu yang telah diedit: 02 Oktober 2020, 17.26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3-outposts:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "datasync:ListTasks",
        "datasync:ListLocations",
        "datasync:DescribeTask",
        "datasync:DescribeLocation*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:ListOutposts",
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonS3OutpostsReadOnlyAccess

`AmazonS3OutpostsReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Amazon S3 di Outposts melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonS3OutpostsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 02 Oktober 2020, 18:55 UTC
- Waktu yang telah diedit: 02 Oktober 2020, 18.55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3-outposts:Get*",
        "s3-outposts:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:ListTasks",
        "datasync:ListLocations",
        "datasync:DescribeTask",
```

```
        "datasync:DescribeLocation*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:ListOutposts",
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonS3ReadOnlyAccess

`AmazonS3ReadOnlyAccess`adalah sebuahAWSkebijakan terkelolaitu: Menyediakan akses baca saja ke semua ember melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonS3ReadOnlyAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Tipe:AWSkebijakan terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang diedit:10 Agustus 2023, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3(default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber dayaAWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai denganAWSkebijakan terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

`AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan peran layanan yang digunakan oleh layananLayanan AWS Katalog untuk menyediakan produk dari SageMaker portofolio produk Amazon. Memberikan izin untuk serangkaian layanan terkait termasuk CodePipeline,, CodeBuild CodeCommit, Glue CloudFormation, dll,.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 November 2020, 18:48 UTC
- Waktu yang telah diedit: 02 Agustus 2022, 19.12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:PATCH",
        "apigateway:DELETE"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:POST"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:launch-source"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:PATCH"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
```

```
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*",
      "Condition" : {
        "ArnLikeIfExists" : {
          "cloudformation:RoleArn" : [
            "arn:aws:sts::*:assumed-role/AmazonSageMakerServiceCatalog*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:UpdateProject"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CreateCommit",
        "codecommit:CreateRepository",
```

```
        "codecommit:DeleteRepository",
        "codecommit:GetRepository",
        "codecommit:TagResource"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codepipeline:CreatePipeline",
        "codepipeline:DeletePipeline",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:StartPipelineExecution",
        "codepipeline:TagResource",
        "codepipeline:UpdatePipeline"
      ],
      "Resource" : [
        "arn:aws:codepipeline:*:*:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:CreateUserPool",
        "cognito-idp:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:launch-source"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:CreateGroup",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteGroup",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:DeleteUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:DeleteRepository",
        "ecr:TagResource"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DeleteRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
```

```
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:CreateDeliveryStream",
        "firehose:DeleteDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "firehose:StartDeliveryStreamEncryption",
        "firehose:StopDeliveryStreamEncryption",
        "firehose:UpdateDestination"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker-*",
        "arn:aws:glue:*:*:table/sagemaker-*",
        "arn:aws:glue:*:*:userDefinedFunction/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateClassifier",
        "glue:DeleteClassifier",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeleteTrigger",
        "glue:DeleteWorkflow",
        "glue:StopCrawler"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateWorkflow"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:workflow/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateJob"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:job/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCrawler",
        "glue:GetCrawler"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:crawler/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTrigger",
        "glue:GetTrigger"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:trigger/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerServiceCatalog*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "lambda:TagResource",
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutRetentionPolicy"
      ],
```

```
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/apigateway/AccessLogs/*",
        "arn:aws:logs:*:*:log-group::log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:GetBucketPolicy",
        "s3:PutBucketAcl",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketCORS",
        "s3:PutBucketTagging",
        "s3:PutObjectTagging"
      ],
      "Resource" : "arn:aws:s3:::sagemaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeWorkteam",
        "sagemaker:CreateCodeRepository",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:DeleteCodeRepository"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:CreateImage",
        "sagemaker:DeleteImage",
        "sagemaker:DescribeImage",
        "sagemaker:UpdateImage",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:image/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "states:CreateStateMachine",
        "states:DeleteStateMachine",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSageMakerCanvasAIServicesAccess

`AmazonSageMakerCanvasAIServicesAccess`adalah kebijakan AWS terkelola yang: Memberikan izin bagi Amazon SageMaker Canvas untuk menggunakan layanan AI guna mendukung solusi AI yang siap digunakan. Kebijakan ini akan menambahkan lebih banyak izin bermutasi untuk layanan saat Amazon SageMaker Canvas menambahkan dukungan.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasAIServicesAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 23 Maret 2023, 22:36 UTC
- Waktu telah diedit: 29 November 2023, 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Textract",
      "Effect" : "Allow",
      "Action" : [
        "textract:AnalyzeDocument",
        "textract:AnalyzeExpense",
        "textract:AnalyzeID",
```

```
        "textract:StartDocumentAnalysis",
        "textract:StartExpenseAnalysis",
        "textract:GetDocumentAnalysis",
        "textract:GetExpenseAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Rekognition",
      "Effect" : "Allow",
      "Action" : [
        "rekognition:DetectLabels",
        "rekognition:DetectText"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Comprehend",
      "Effect" : "Allow",
      "Action" : [
        "comprehend:BatchDetectDominantLanguage",
        "comprehend:BatchDetectEntities",
        "comprehend:BatchDetectSentiment",
        "comprehend:DetectPiiEntities",
        "comprehend:DetectEntities",
        "comprehend:DetectSentiment",
        "comprehend:DetectDominantLanguage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Bedrock",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:ListFoundationModels",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateBedrockResourcesPermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "bedrock:CreateModelCustomizationJob",
        "bedrock:CreateProvisionedModelThroughput",
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:model-customization-job/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker",
            "Canvas"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:RequestTag/Canvas" : "true",
          "aws:ResourceTag/SageMaker" : "true",
          "aws:ResourceTag/Canvas" : "true"
        }
      }
    },
    {
      "Sid" : "GetStopAndDeleteBedrockResourcesPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetCustomModel",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:StopModelCustomizationJob",
        "bedrock:DeleteProvisionedModelThroughput"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:model-customization-job/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true",
          "aws:ResourceTag/Canvas" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "FoundationModelPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelCustomizationJob"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "BedrockFineTuningPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerCanvasBedrockAccess

`AmazonSageMakerCanvasBedrockAccess`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin untuk menggunakan Amazon Bedrock di SageMaker Canvas dengan menyediakan akses ke layanan hilir seperti S3.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasBedrockAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Februari 2024, 18:37 UTC
- Waktu telah diedit: 02 Februari 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3CanvasAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/Canvas",
        "arn:aws:s3:::sagemaker-*/Canvas/*"
      ]
    },
    {
      "Sid" : "S3BucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerCanvasDataPrepFullAccess

`AmazonSageMakerCanvasDataPrepFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke SageMaker sumber daya dan operasi Amazon untuk persiapan data di Canvas. Kebijakan ini juga menyediakan akses tertentu ke layanan terkait (misalnya, S3, IAM, KMS, RDS, Log, Redshift, Athena CloudWatch , Glue,, Secrets Manager). EventBridge Kebijakan ini harus dilampirkan ke peran eksekusi SageMaker Domain/Profil Pengguna Amazon.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasDataPrepFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Oktober 2023, 22:56 UTC
- Waktu telah diedit: 08 Desember 2023, 02:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerListFeatureGroupOperation",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListFeatureGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerFeatureGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateFeatureGroup",
        "sagemaker:DescribeFeatureGroup"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:feature-group/*"
    },
    {
      "Sid" : "SageMakerProcessingJobOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateProcessingJob",
```

```
        "sagemaker:DescribeProcessingJob",
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:processing-job/*canvas-data-prep*"
    },
    {
      "Sid" : "SageMakerProcessingJobListOperation",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListProcessingJobs",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPipelineOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribePipeline",
        "sagemaker:CreatePipeline",
        "sagemaker:UpdatePipeline",
        "sagemaker:DeletePipeline",
        "sagemaker:StartPipelineExecution",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:DescribePipelineExecution"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:pipeline/*canvas-data-prep*"
    },
    {
      "Sid" : "KMSListOperations",
      "Effect" : "Allow",
      "Action" : "kms:ListAliases",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
```

```
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetObjectOperation",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMListOperations",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "IAMGetOperations",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassOperation",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EventBridgePutOperation",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "EventBridgeTagBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTagOperation",
      "Effect" : "Allow",
      "Action" : "events:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:SearchTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "EMROperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups"
```

```
      ],
      "Resource" : "arn:aws:elasticmapreduce:*:*:cluster/*"
    },
    {
      "Sid" : "EMRListOperation",
      "Effect" : "Allow",
      "Action" : "elasticmapreduce:ListClusters",
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaListDataCatalogOperation",
      "Effect" : "Allow",
      "Action" : "athena:ListDataCatalogs",
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaQueryExecutionOperations",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*"
    },
    {
      "Sid" : "AthenaDataCatalogOperations",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*"
    },
    {
      "Sid" : "RedshiftOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "RedshiftArnBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "arn:aws:redshift:*:*:cluster:*"
    },
    {
      "Sid" : "RedshiftGetCredentialsOperation",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "SecretsManagerARNBasedOperation",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
    },
    {
      "Sid" : "SecretManagerTagBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
```

```
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "LoggingOperation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/studio:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerCanvasDirectDeployAccess

`AmazonSageMakerCanvasDirectDeployAccess`adalah kebijakan AWS terkelola yang: Mengizinkan Amazon SageMaker Canvas membuat, mengelola, dan melihat detail titik akhir untuk titik akhir yang dibuat melalui Canvas. Memungkinkan Amazon SageMaker Canvas untuk mengambil metrik pemanggilan titik akhir dari. CloudWatch

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasDirectDeployAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Oktober 2023, 18:11 UTC

- Waktu telah diedit: 06 Oktober 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerEndpointPerms",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:InvokeEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:Canvas*",
        "arn:aws:sagemaker:*:*:canvas*"
      ]
    },
    {
      "Sid" : "ReadCWInvocationMetrics",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerCanvasForecastAccess

`AmazonSageMakerCanvasForecastAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin yang biasanya diperlukan untuk menggunakan SageMaker Canvas dengan Amazon Forecast.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerCanvasForecastAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 24 Agustus 2022, 20:04 UTC
- Waktu yang telah diedit: 24 Agustus 2022, 20.04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/Canvas*",
        "arn:aws:s3:::sagemaker-*/canvas*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSageMakerCanvasFullAccess

`AmazonSageMakerCanvasFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke sumber daya dan operasi Amazon SageMaker Canvas. Kebijakan ini juga menyediakan

akses tertentu ke layanan terkait (misalnya, S3, IAM, VPC, ECR, Logs, Redshift, Secrets Manager CloudWatch , dan Forecast). Kebijakan ini harus dilampirkan ke peran eksekusi SageMaker Domain/ Profil Pengguna Amazon.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerCanvasFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 09 September 2022, 00:44 UTC
- Waktu telah diedit: 24 Januari 2024, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerUserDetailsAndPackageOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListTags",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListEndpoints"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPackageGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelPackage"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*"
      ]
    },
    {
      "Sid" : "SageMakerTrainingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:AddTags",
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*Canvas*",
        "arn:aws:sagemaker:*:*:*canvas*",
        "arn:aws:sagemaker:*:*:*model-compilation-*"
      ]
```

```
    },
    {
      "Sid" : "SageMakerHostingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteModel",
        "sagemaker:InvokeEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:InvokeEndpointAsync"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*Canvas*",
        "arn:aws:sagemaker:*:*:*canvas*"
      ]
    },
    {
      "Sid" : "EC2VPCOperation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECROperations",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetOperations",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassOperation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LoggingOperation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:CreateBucket",
        "s3:GetBucketCors",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
```

```
      "Sid" : "ReadSageMakerJumpstartArtifacts",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
      ]
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : "glue:SearchTables",
      "Resource" : [
        "arn:aws:glue:*:*:table/*/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "SecretsManagerARNBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
```

```
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "SecretManagerTagBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftGetCredentialsOperation",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
```

```
      "Sid" : "ForecastOperations",
      "Effect" : "Allow",
      "Action" : [
        "forecast:CreateExplainabilityExport",
        "forecast:CreateExplainability",
        "forecast:CreateForecastEndpoint",
        "forecast:CreateAutoPredictor",
        "forecast:CreateDatasetImportJob",
        "forecast:CreateDatasetGroup",
        "forecast:CreateDataset",
        "forecast:CreateForecast",
        "forecast:CreateForecastExportJob",
        "forecast:CreatePredictorBacktestExportJob",
        "forecast:CreatePredictor",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeExplainability",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeForecastEndpoint",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeDataset",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:GetAccuracyMetrics",
        "forecast:InvokeForecastEndpoint",
        "forecast:GetRecentForecastContext",
        "forecast:DescribePredictor",
        "forecast:TagResource",
        "forecast:DeleteResourceTree"
      ],
      "Resource" : [
        "arn:aws:forecast:*:*:*Canvas*"
      ]
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassOperationForForecast",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AutoscalingOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "sagemaker",
          "application-autoscaling:scalable-dimension" :
"sagemaker:variant:DesiredInstanceCount"
        }
      }
    },
    {
      "Sid" : "AsyncEndpointOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "sagemaker:DescribeEndpointConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerCloudWatchUpdate",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AutoscalingSageMakerEndpointOperation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerClusterInstanceRolePolicy

`AmazonSageMakerClusterInstanceRolePolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin yang biasanya diperlukan untuk menggunakan Amazon SageMaker Cluster.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerClusterInstanceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2023, 15:11 UTC
- Waktu telah diedit: 29 November 2023, 15:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudwatchLogStreamPublishPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*:log-stream:*"
      ]
    },
    {
      "Sid" : "CloudwatchLogGroupCreationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*"
```

```
      ]
    },
    {
      "Sid" : "CloudwatchPutMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "/aws/sagemaker/Clusters"
        }
      }
    },
    {
      "Sid" : "DataRetrievalFromS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SSMConnectivityPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerCoreServiceRolePolicy

`AmazonSageMakerCoreServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan terkelola untuk Peran Tertaut Layanan untuk Amazon SageMaker Core Services

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, peran Anda.

detail kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Desember 2020, 21:40 UTC
- Waktu yang telah diedit: 21 Desember 2020, 21.40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:AuthorizedService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSageMakerEdgeDeviceFleetPolicy

`AmazonSageMakerEdgeDeviceFleetPolicy`adalah kebijakanAWS terkelola yang: Menyediakan izin yang diperlukan bagi SageMaker Edge untuk membuat dan mengelola armada perangkat untuk pelanggan menggunakan koneksi cloud default.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerEdgeDeviceFleetPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 08 Desember 2020, 16:17 UTC
- Waktu yang telah diedit: 08 Desember 2020, 16.17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "DeviceS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "SageMakerEdgeApis",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:SendHeartbeat",
        "sagemaker:GetDeviceRegistration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateIoTRoleAlias",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateRoleAlias",
        "iot:DescribeRoleAlias",
        "iot:UpdateRoleAlias",
        "iot:ListTagsForResource",
        "iot:TagResource"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:rolealias/SageMakerEdge*"
      ]
    },
    {
      "Sid" : "CreateIoTRoleAliasIamPermissionsGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*",
```

```
        "arn:aws:iam::*:role/*Sagemaker*",
        "arn:aws:iam::*:role/*sagemaker*"
      ]
    },
    {
      "Sid" : "CreateIoTRoleAliasIamPermissionsPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*",
        "arn:aws:iam::*:role/*Sagemaker*",
        "arn:aws:iam::*:role/*sagemaker*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com",
            "credentials.iot.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSageMakerFeatureStoreAccess

`AmazonSageMakerFeatureStoreAccess`adalah kebijakanAWS terkelola yang: Menyediakan izin yang diperlukan untuk mengaktifkan toko offline untuk grup SageMaker FeatureStore fitur Amazon.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerFeatureStoreAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Desember 2020, 16:24 UTC
- Waktu yang telah diedit: 05 Desember 2022, 14.19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*/metadata/*",
        "arn:aws:s3:::*Sagemaker*/metadata/*",
        "arn:aws:s3:::*sagemaker*/metadata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSageMakerFullAccess

`AmazonSageMakerFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke Amazon SageMaker melalui AWS Management Console dan SDK. Juga menyediakan akses pilih ke layanan terkait (misalnya, S3, ECR, CloudWatch Log).

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSageMakerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2017, 13:07 UTC
- Waktu telah diedit: 30 November 2023, 13:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFullAccess`

Versi kebijakan

Versi kebijakan: v25 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Sid" : "AllowAddTagsForApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
```

```
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*"
      ]
    },
    {
      "Sid" : "AllowStudioActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListUserProfiles",
        "sagemaker:DescribeSpace",
        "sagemaker:ListSpaces",
        "sagemaker:DescribeApp",
        "sagemaker:ListApps"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppActionsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAppActionsForSharedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private",
            "Shared"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowFlowDefinitionActions",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
```

```
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "cognito-idp:AdminAddUserToGroup",
        "cognito-idp:AdminCreateUser",
        "cognito-idp:AdminDeleteUser",
        "cognito-idp:AdminDisableUser",
        "cognito-idp:AdminEnableUser",
        "cognito-idp:AdminRemoveUserFromGroup",
        "cognito-idp:CreateGroup",
        "cognito-idp:CreateUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:List*",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:CreateRepository",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:StartImageScan",
        "elastic-inference:Connect",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "glue:CreateJob",
        "glue:DeleteJob",
        "glue:GetJob*",
        "glue:GetTable*",
        "glue:GetWorkflowRun",
        "glue:ResetJobBookmark",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:UpdateJob",
        "groundtruthlabeling:*",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery",
        "robomaker:CreateSimulationApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:DeleteSimulationApplication",
        "robomaker:CreateSimulationJob",
        "robomaker:DescribeSimulationJob",
        "robomaker:CancelSimulationJob",
```

```
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowECRActions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeCommitActions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:*sagemaker*",
        "arn:aws:codecommit:*:*:*SageMaker*",
        "arn:aws:codecommit:*:*:*Sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeBuildActions",
      "Action" : [
```

```
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker*",
        "arn:aws:codebuild:*:*:build/*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowStepFunctionsActions",
      "Action" : [
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:statemachine:*sagemaker*",
        "arn:aws:states:*:*:execution:*sagemaker*:*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowSecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "AllowReadOnlySecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowServiceCatalogProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ProvisionProduct"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*",
        "arn:aws:s3:::*aws-glue*"
      ]
    },
```

```
    {
      "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowS3BucketACL",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowLambdaInvokeFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForRobomaker",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSNSActions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForSageMakerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonSageMaker*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "robomaker.amazonaws.com",
            "states.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAthenaActions",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueCreateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueUpdateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore"
      ]
```

```
    },
    {
      "Sid" : "AllowGlueDeleteTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetTablesAndDatabases",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetAndCreateDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:database/sagemaker_processing",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/sagemaker_data_wrangler"
      ]
    },
    {
      "Sid" : "AllowRedshiftDataActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowRedshiftGetClusterCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowListTagsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*"
      ]
    },
    {
      "Sid" : "AllowCloudformationListStackResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AllowS3ExpressObjectActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateSession"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*",
        "arn:aws:s3express:*:*:bucket/*aws-glue*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressCreateBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressListBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:ListAllMyDirectoryBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSageMakerGeospatialExecutionRole

`AmazonSageMakerGeospatialExecutionRole`adalah kebijakanAWS terkelola yang: Kebijakan ini menyediakan akses ke layanan yang umumnya dibutuhkan untuk menggunakanSageMaker geospasial.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerGeospatialExecutionRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 30 November 2022, 10:08 UTC
- Waktu yang telah diedit: 10 Mei 2023, 20.28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:GetEarthObservationJob",
      "Resource" : "arn:aws:sagemaker-geospatial:*:*:earth-observation-job/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:GetRasterDataCollection",
      "Resource" : "arn:aws:sagemaker-geospatial:*:*:raster-data-collection/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSageMakerGeospatialFullAccess

`AmazonSageMakerGeospatialFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin yang memungkinkan akses penuh ke Amazon SageMaker Geospasial melaluiAWS Management Console dan SDK.

Menggunakan kebijakan

Anda dapat melampirkan`AmazonSageMakerGeospatialFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 30 November 2022, 10:06 UTC
- Waktu yang telah diedit: 30 November 2022, 10.06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker-geospatial.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSageMakerGroundTruthExecution

`AmazonSageMakerGroundTruthExecution`adalah kebijakanAWS terkelola yang: Menyediakan akses keAWS layanan yang diperlukan untuk menjalankan pekerjaan SageMaker GroundTruth Pelabelan

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerGroundTruthExecution` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 Juli 2020, 19:30 UTC
- Waktu yang telah diedit: 29 April 2022 20.49 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CustomLabelingJobs",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*GtRecipe*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*",
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*GroundTruth*",
        "arn:aws:s3:::*Groundtruth*",
        "arn:aws:s3:::*groundtruth*",
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
```

```
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StreamingQueue",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
```

```
        "sqs:SendMessage",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : "arn:aws:sqs:*:*:*GroundTruth*"
    },
    {
      "Sid" : "StreamingTopicSubscribe",
      "Effect" : "Allow",
      "Action" : "sns:Subscribe",
      "Resource" : [
        "arn:aws:sns:*:*:*GroundTruth*",
        "arn:aws:sns:*:*:*Groundtruth*",
        "arn:aws:sns:*:*:*groundTruth*",
        "arn:aws:sns:*:*:*groundtruth*",
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sageMaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sns:Protocol" : "sqs"
        },
        "StringLike" : {
          "sns:Endpoint" : "arn:aws:sqs:*:*:*GroundTruth*"
        }
      }
    },
    {
      "Sid" : "StreamingTopic",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*GroundTruth*",
        "arn:aws:sns:*:*:*Groundtruth*",
        "arn:aws:sns:*:*:*groundTruth*",
        "arn:aws:sns:*:*:*groundtruth*",
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sageMaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
```

```
    },
    {
      "Sid" : "StreamingTopicUnsubscribe",
      "Effect" : "Allow",
      "Action" : [
        "sns:Unsubscribe"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "WorkforceVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ec2:VpceServiceName" : [
            "*sagemaker-task-resources*",
            "aws.sagemaker*labeling*"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSageMakerMechanicalTurkAccess

`AmazonSageMakerMechanicalTurkAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk membuat FlowDefinition sumber daya Amazon Augmented AI terhadap Workteam mana pun.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerMechanicalTurkAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 Desember 2019, 16:19 UTC
- Waktu yang telah diedit: 03 Desember 2019 16.19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSageMakerModelGovernanceUseAccess

`AmazonSageMakerModelGovernanceUseAccess`adalahAWSkebijakan terkelolabahwa: IniAWSkebijakan terkelola memberikan izin yang diperlukan untuk menggunakan semua AmazonSageMakerFitur tata kelola. Kebijakan ini juga menyediakan akses pilih ke layanan terkait (misalnya, S3, KMS).

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerModelGovernanceUseAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 30 November 2022, 08:58 UTC
- Waktu yang diedit:17 Juli 2023, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess`

Versi kebijakan

Versi kebijakan: v2(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:UpdateMonitoringAlert",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:ListMonitoringAlertHistory",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:CreateModelCard",
        "sagemaker:DescribeModelCard",
        "sagemaker:UpdateModelCard",
        "sagemaker:DeleteModelCard",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelCardVersions",
        "sagemaker:CreateModelCardExportJob",
        "sagemaker:DescribeModelCardExportJob",
        "sagemaker:ListModelCardExportJobs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTrainingJobs",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:ListModels",
        "sagemaker:DescribeModel",
        "sagemaker:Search",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags",
        "sagemaker:ListTags"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:CreateBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSageMakerModelRegistryFullAccess

`AmazonSageMakerModelRegistryFullAccess`adalah kebijakanAWS terkelola yang: Ini adalah kebijakan terkelola baru untuk Model Registry di Sagemaker. Kebijakan ini adalah kebijakan mandiri yang dapat dilampirkan ke peran pengguna untuk mengakses fungsi terkait Model Registry di Sagemaker.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerModelRegistryFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 13 April 2023, 05:20 UTC
- Waktu yang telah diedit: 13 April 2023, 05:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeAction",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
```

```
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:ListAssociations",
        "sagemaker:ListArtifacts",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackages",
        "sagemaker:Search",
        "sagemaker:GetSearchSuggestions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteTags",
        "sagemaker:UpdateModelPackage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:DescribeImages"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "sagemaker:collection"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:DeleteGroup",
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:collection" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSageMakerNotebooksServiceRolePolicy

`AmazonSageMakerNotebooksServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan terkelola untuk Peran Tertaut Layanan untuk SageMaker Notebook Amazon

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran baru.

Detail kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 Oktober 2019, 20:27 UTC
- Waktu yang telah diedit: 09 Maret 2023, 18.20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateAccessPoint",
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*",
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "elasticfilesystem:DeleteAccessPoint"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:access-point/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateFileSystem",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:TagResource",
      "Resource" : [
        "arn:aws:elasticfilesystem:*:*:access-point/*",
        "arn:aws:elasticfilesystem:*:*:file-system/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
```

```
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateManagedApplicationInstance",
        "sso:DeleteManagedApplicationInstance",
        "sso:GetManagedApplicationInstance"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceR

`AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`adalahAWS terkelolabahwa: Kebijakan peran layanan yang digunakan olehAWSApigateway dalamAWS ServiceCatalogproduk yang disediakan dari AmazonSageMakerportofolio produk. Memberikan izin untuk serangkaian layanan terkait termasuk Lambda dan lainnya.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy` pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Agustus 2023, 15:06 UTC
- Waktu yang diedit:01 Agustus 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:sagemaker-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker:InvokeEndpoint",
      "Resource" : "arn:aws:sagemaker:*:*:endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServ

`AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`adalah sebuahAWSkebijakan terkelolabahwa: Kebijakan peran layanan yang digunakan olehAWS CloudFormationdalamAWS ServiceCatalogproduk yang disediakan dari AmazonSageMakerportofolio produk. Memberikan izin kepada subset layanan terkait termasuk Lambda, Apigateway, dan lainnya.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePo` pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Agustus 2023, 15:06 UTC
- Waktu yang diedit:01 Agustus 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1(default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsLambdaRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsApiGatewayRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "apigateway.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:DeleteFunction",
        "lambda:UpdateFunctionCode",
        "lambda:ListTags",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "ForAnyValue:StringEquals" : {
```

```
          "aws:TagKeys" : [
            "sagemaker:project-name",
            "sagemaker:partner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PublishLayerVersion",
        "lambda:GetLayerVersion",
        "lambda:DeleteLayerVersion",
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:layer:sagemaker-*",
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:POST",
```

```
        "apigateway:PUT"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name",
            "sagemaker:partner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/lambda-auth-code/layer.zip"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai denganAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRoleP

`AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`adalahAWSkebija terkelolabahwa: Kebijakan peran layanan yang digunakan olehAWSLambda dalamAWS ServiceCatalogproduk yang disediakan dari AmazonSageMakerportofolio produk. Memberikan izin untuk serangkaian layanan terkait termasuk Manajer Rahasia dan lainnya.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Agustus 2023, 15:05 UTC
- Waktu yang diedit:01 Agustus 2023, 15:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/sagemaker:partner" : false
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSageMakerPipelinesIntegrations

`AmazonSageMakerPipelinesIntegrations`adalah kebijakanAWS terkelola yang: Kebijakan Terkelola Amazon ini memberikan izin yang biasanya diperlukan untuk digunakan dengan langkah-langkah Callback dan langkah-langkah Lambda di Jalur Pipa Pembuatan SageMaker Model. Hal ini ditambahkan ke AmazonSageMaker -ExecutionRole yang dapat dibuat saat mengatur SageMaker Studio. Hal ini juga dapat dilampirkan ke peran lain yang akan digunakan untuk authoring atau mengeksekusi jaringan pipa.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerPipelinesIntegrations` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 Juli 2021, 16:35 UTC
- Waktu yang telah diedit: 17 Februari 2023, 21.28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*sageMaker*",
        "arn:aws:lambda:*:*:function:*SageMaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:*sagemaker*",
        "arn:aws:sqs:*:*:*sageMaker*",
        "arn:aws:sqs:*:*:*SageMaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/SageMakerPipelineExecutionEMRStepStatusUpdateRule",
        "arn:aws:events:*:*:rule/SageMakerPipelineExecutionEMRClusterStatusUpdateRule"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:RunJobFlow",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:ListSteps"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSageMakerReadOnly

`AmazonSageMakerReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Amazon SageMaker melaluiAWS Management Console dan SDK.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 November 2017, 13:07 UTC
- Waktu yang telah diedit: 01 Desember 2021 16.29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerReadOnly`

Versi kebijakan

Versi kebijakan:v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sagemaker:BatchGetMetrics",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:BatchGetRecord",
        "sagemaker:GetRecord",
        "sagemaker:Search",
        "sagemaker:QueryLineage",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:GetModelPackageGroupPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "aws-marketplace:ViewSubscriptions",
        "cloudwatch:DescribeAlarms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListUsersInGroup",
        "ecr:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePoli

`AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan peran layanan yang digunakan olehAWS ApigateWay dalam produkAWS ServiceCatalog yang disediakan dari SageMaker portofolio produk Amazon. Memberikan izin untuk serangkaian layanan terkait termasuk CloudWatch Log dan lainnya.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 25 Maret 2022, 04:25 UTC
- Waktu yang telah diedit: 25 Maret 2022, 04.25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/apigateway/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSageMakerServiceCatalogProductsCloudformationServiceRoleP

`AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan peran layanan yang digunakan olehAWS CloudFormation dalam produkAWS ServiceCatalog yang disediakan dari SageMaker portofolio produk Amazon. Memberikan izin kepada subset layanan terkait termasuk SageMaker dan lainnya.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 25 Maret 2022, 04:26 UTC
- Waktu yang telah diedit: 25 Maret 2022, 04:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
```

```
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
```

```
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
```

```
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
```

```
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
```

```
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
```

```
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "NotResource" : [
```

```
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

`AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan peran layanan yang digunakan olehAWS CodeBuild dalam produkAWS ServiceCatalog yang disediakan dari SageMaker portofolio produk Amazon. Memberikan izin kepada subset layanan terkait termasuk CodePipeline, CodeBuild dan lainnya.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 25 Maret 2022, 04:27 UTC
- Waktu yang telah diedit: 25 Maret 2022, 04.27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeImageReplicationStatus",
        "ecr:DescribeRepositories",
        "ecr:DescribeImageReplicationStatus",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsEventsRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodePipelineRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "events.amazonaws.com",
            "codepipeline.amazonaws.com",
            "cloudformation.amazonaws.com",
            "codebuild.amazonaws.com",
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
```

```
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
```

```
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
```

```
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
```

```
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
```

```
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
```

```
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
```

```
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

`AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan peran layanan yang digunakan olehAWS CodePipeline dalam produkAWS ServiceCatalog yang disediakan dari SageMaker portofolio produk Amazon. Memberikan izin kepada subset layanan terkait termasuk CodePipeline, CodeBuild dan lainnya.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 Februari 2022, 09:53 UTC
- Waktu yang telah diedit: 22 Februari 2022, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
```

```
        "cloudformation:DescribeChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*",
        "arn:aws:codebuild:*:*:build/sagemaker-*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

`AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan peran layanan yang digunakan olehAWS CloudWatch Acara dalam produkAWS ServiceCatalog yang disediakan dari SageMaker portofolio produk Amazon. Memberikan izin kepada subset layanan terkait termasuk CodePipeline dan lainnya.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 Februari 2022, 09:53 UTC

- Waktu yang telah diedit: 22 Februari 2022, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "codepipeline:StartPipelineExecution",
      "Resource" : "arn:aws:codepipeline:*:*:sagemaker-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

`AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan peran layanan yang digunakan olehAWS Firehose dalam

produkAWS ServiceCatalog yang disediakan dari SageMaker portofolio produk Amazon. Memberikan izin untuk serangkaian layanan terkait termasuk Firehose dan lainnya.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 Februari 2022, 09:54 UTC
- Waktu yang telah diedit: 22 Februari 2022, 09:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

`AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan peran layanan yang digunakan olehAWS Glue dalam produkAWS ServiceCatalog yang disediakan dari SageMaker portofolio produk Amazon. Memberikan izin untuk serangkaian layanan terkait termasuk Glue, S3, dan lainnya.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 22 Februari 2022, 09:51 UTC
- Waktu yang telah diedit: 26 Agustus 2022, 19.13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetPartition",
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:DeletePartition",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:GetDatabase",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:SearchTables",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/global_temp",
        "arn:aws:glue:*:*:database/sagemaker-*",
        "arn:aws:glue:*:*:table/sagemaker-*",
        "arn:aws:glue:*:*:tableVersion/sagemaker-*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
```

```
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/glue/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

`AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan peran layanan yang digunakan olehAWS Lambda dalam produk yangAWS ServiceCatalog disediakan dari SageMaker portofolio produk Amazon. Memberikan izin untuk serangkaian layanan terkait termasuk ECR, S3, dan lainnya.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 04 April 2022, 16:34 UTC
- Waktu yang telah diedit: 04 April 2022, 16.34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeImages",
        "ecr:BatchDeleteImage",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:DeleteRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
```

```
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
```

```
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
```

```
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
```

```
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
```

```
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
```

```
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:action/*",
        "arn:aws:sagemaker:*:*:algorithm/*",
        "arn:aws:sagemaker:*:*:app-image-config/*",
        "arn:aws:sagemaker:*:*:artifact/*",
        "arn:aws:sagemaker:*:*:automl-job/*",
        "arn:aws:sagemaker:*:*:code-repository/*",
        "arn:aws:sagemaker:*:*:compilation-job/*",
        "arn:aws:sagemaker:*:*:context/*",
```

```
        "arn:aws:sagemaker:*:*:data-quality-job-definition/*",
        "arn:aws:sagemaker:*:*:device-fleet/*/device/*",
        "arn:aws:sagemaker:*:*:device-fleet/*",
        "arn:aws:sagemaker:*:*:edge-packaging-job/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:experiment/*",
        "arn:aws:sagemaker:*:*:experiment-trial/*",
        "arn:aws:sagemaker:*:*:experiment-trial-component/*",
        "arn:aws:sagemaker:*:*:feature-group/*",
        "arn:aws:sagemaker:*:*:human-loop/*",
        "arn:aws:sagemaker:*:*:human-task-ui/*",
        "arn:aws:sagemaker:*:*:hyper-parameter-tuning-job/*",
        "arn:aws:sagemaker:*:*:image/*",
        "arn:aws:sagemaker:*:*:image-version/*/*",
        "arn:aws:sagemaker:*:*:inference-recommendations-job/*",
        "arn:aws:sagemaker:*:*:labeling-job/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:model-bias-job-definition/*",
        "arn:aws:sagemaker:*:*:model-explainability-job-definition/*",
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*",
        "arn:aws:sagemaker:*:*:model-quality-job-definition/*",
        "arn:aws:sagemaker:*:*:monitoring-schedule/*",
        "arn:aws:sagemaker:*:*:notebook-instance/*",
        "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:pipeline/*/execution/*",
        "arn:aws:sagemaker:*:*:processing-job/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:training-job/*",
        "arn:aws:sagemaker:*:*:transform-job/*",
        "arn:aws:sagemaker:*:*:workforce/*",
        "arn:aws:sagemaker:*:*:workteam/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSecurityLakeAdministrator

`AmazonSecurityLakeAdministrator`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke Amazon Security Lake dan layanan terkait yang diperlukan untuk mengelola Security Lake.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSecurityLakeAdministrator` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Mei 2023, 22:04 UTC
- Waktu telah diedit: 23 Februari 2024, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowActionsWithAnyResource",
      "Effect" : "Allow",
      "Action" : [
        "securitylake:*",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListAccounts",
        "iam:ListRoles",
        "ram:GetResourceShareAssociations"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsWithAnyResourceViaSecurityLake",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCrawler",
        "glue:StopCrawlerSchedule",
        "lambda:CreateEventSourceMapping",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:GetDatalakeSettings",
        "events:ListConnections",
        "events:ListApiDestinations",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowManagingSecurityLakeS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketNotification",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketVersioning",
        "s3:PutReplicationConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetBucketNotification"
```

```
      ],
      "Resource" : "arn:aws:s3:::aws-security-data-lake*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowLambdaCreateFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowLambdaAddPermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        },
        "StringEquals" : {
          "lambda:Principal" : "securitylake.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase",
        "glue:CreateTable",
        "glue:GetTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DescribeRule",
        "events:CreateApiDestination",
        "events:CreateConnection",
        "events:UpdateConnection",
        "events:UpdateApiDestination",
        "events:DeleteConnection",
        "events:DeleteApiDestination",
        "events:ListTargetsByRule",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AmazonSecurityLake*",
        "arn:aws:events:*:*:rule/SecurityLake*",
        "arn:aws:events:*:*:api-destination/AmazonSecurityLake*",
        "arn:aws:events:*:*:connection/AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSQSActions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes",
        "sqs:GetQueueURL",
        "sqs:AddPermission",
        "sqs:GetQueueAttributes",
        "sqs:DeleteQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:SecurityLake*",
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsCmkGrantForSecurityLake",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::aws-security-data-lake*"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "GenerateDataKey",
            "RetireGrant",
            "Decrypt"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AllowEnablingQueryBasedSubscribers",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare",
        "ram:AssociateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:ResourceArn" : [
            "arn:aws:glue:*:*:catalog",
            "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
            "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowConfiguringQueryBasedSubscribers",
      "Effect" : "Allow",
      "Action" : [
        "ram:UpdateResourceShare",
        "ram:GetResourceShares",
        "ram:DisassociateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : "LakeFormation*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowConfiguringCredentialsForSubscriberNotification",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/
AmazonSecurityLake-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForUpdatingGluePartitionsSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForUpdatingGluePartitionsLambdaArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        },
        "StringLike" : {
```

```
          "iam:AssociatedResourceARN" : [
            "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
            "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCrossRegionReplicationSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "s3.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCrossRegionReplicationS3Arn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "s3.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:s3:::aws-security-data-lake*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "AllowPassRoleForCustomSourceCrawlerSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCustomSourceCrawlerGlueArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForSubscriberNotificationSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "events.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:subscriber/*"
        }
      }
    },
```

```
    {
      "Sid" : "AllowPassRoleForSubscriberNotificationEventsArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "events.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:events:*:*:rule/AmazonSecurityLake*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowOnboardingToSecurityLakeDependencies",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/securitylake.amazonaws.com/
AWSServiceRoleForSecurityLake",
        "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
        "arn:aws:iam::*:role/aws-service-role/apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "securitylake.amazonaws.com",
            "lakeformation.amazonaws.com",
            "apidestinations.events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowRolePolicyActionsforSubscibersandSources",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonSecurityLakePermissionsBoundary"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowRegisterS3LocationInLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PutRolePolicy",
        "iam:GetRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowIAMActionsByResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRolePolicies",
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "S3ReadAccessToSecurityLakes",
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource" : "arn:aws:s3:::aws-security-data-lake-*"
    },
    {
      "Sid" : "S3ReadAccessToSecurityLakeMetastoreObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::security-lake-meta-store-manager-*"
    },
    {
      "Sid" : "S3ResourcelessReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSecurityLakeMetastoreManager

`AmazonSecurityLakeMetastoreManager`adalah kebijakan AWS terkelola yang: Kebijakan untuk Amazon SecurityLake meta store manager lambda yang memungkinkan akses ke cloudwatch, S3, Glue, dan SQS.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonSecurityLakeMetastoreManager` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 23 Januari 2024, 15:26 UTC
- Waktu telah diedit: 23 Januari 2024, 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowWriteLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
```

```
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
        "arn:aws:logs:*:*:/aws/lambda/AmazonSecurityLake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowGlueManage",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToReadFromSqs",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataReadWrite",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonSecurityLakePermissionsBoundary

`AmazonSecurityLakePermissionsBoundary`adalah kebijakanAWS terkelola yang: Amazon Security Lake membuat peran IAM untuk sumber kustom pihak ketiga untuk menulis data ke data lake dan bagi pelanggan pihak ketiga untuk menggunakan data dari data lake, dan menggunakan kebijakan ini saat membuat peran ini untuk menentukan batas izin mereka.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSecurityLakePermissionsBoundary` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 November 2022, 14:11 UTC
- Waktu yang telah diedit: 29 November 2022, 14.11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
```

```
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "NotAction" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "NotResource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
```

```
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "NotResource" : "arn:aws:sqs:*:*:AmazonSecurityLake*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringNotLikeIfExists" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::aws-security-data-lake*"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:sqs:arn" : "false"
        },
        "StringNotLikeIfExists" : {
          "kms:EncryptionContext:aws:sqs:arn" : [
            "arn:aws:sqs:*:*:AmazonSecurityLake*"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSESFullAccess

`AmazonSESFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon SES melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSESFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 18.41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSESReadOnlyAccess

`AmazonSESReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Amazon SES melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSESReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 18.41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:Get*",
        "ses:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSNSFullAccess

`AmazonSNSFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon SNS melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSNSFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 18.41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sns:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSNSReadOnlyAccess

`AmazonSNSReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Amazon SNS melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSNSReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 18.41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSNSRole

`AmazonSNSRole`adalah kebijakanAWS terkelola yang: Kebijakan default untuk peran layanan Amazon SNS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSNSRole` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 18.41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSNSRole`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSQSFullAccess

`AmazonSQSFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon SQS melaluiAWS Management Console.

Menggunakan kebijakan

Anda dapat melampirkan`AmazonSQSFullAccess` ke pengguna, grup, dan peran Anda.

Detail

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 18.41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sqs:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSQSReadOnlyAccess

`AmazonSQSReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya baca ke Amazon SQS melalui. AWS Management Console

Menggunakan Kebijakan ini

Anda dapat melampirkan `AmazonSQSReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 15 Juni 2023, 15.37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSSMAutomationApproverAccess

`AmazonSSMAutomationApproverAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk melihat eksekusi otomatisasi dan mengirim keputusan persetujuan yang otomatisasi sedang menunggu persetujuan

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSSMAutomationApproverAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 07 Agustus 2017, 23:07 UTC
- Waktu yang telah diedit: 07 Agustus 2017 23.07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationExecutions",
        "ssm:GetAutomationExecution",
        "ssm:SendAutomationSignal"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSSMAutomationRole

`AmazonSSMAutomationRole`adalah kebijakanAWS terkelola yang: Memberikan izin untuk layanan Otomasi EC2 untuk menjalankan aktivitas yang ditentukan dalam dokumen Otomasi

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSSMAutomationRole` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Desember 2016, 22:09 UTC
- Waktu yang telah diedit: 24 Juli 2017 08.29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default yang menentukan izin untuk kebijakan yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:Automation*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeImages",
```

```
        "ec2:DeleteSnapshot",
        "ec2:StartInstances",
        "ec2:RunInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:Automation*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin IAM yang ditentukan IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSSMDirectoryServiceAccess

`AmazonSSMDirectoryServiceAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memungkinkan Agen SSM untuk mengakses Directory Service atas nama pelanggan untuk domain-bergabung dengan instans terkelola.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSSMDirectoryServiceAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 15 Maret 2019, 17:44 UTC
- Waktu yang telah diedit: 15 Maret 2019 07.44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSSMFullAccess

`AmazonSSMFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon SSM.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSSMFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 Mei 2015, 17:39 UTC
- Waktu yang telah diedit: 20 November 2019, 20.08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMFullAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeInstanceStatus",
        "logs:*",
        "ssm:*",
        "ec2messages:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus menghapus izin
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSSMMaintenanceWindowRole

`AmazonSSMMaintenanceWindowRole`adalah kebijakanAWS terkelola yang: Peran Layanan yang akan digunakan untuk Jendela Pemeliharaan EC2

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSSMMaintenanceWindowRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Desember 2016, 15:57 UTC
- Waktu yang telah diedit: 27 Juli 2019, 00:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SSM*",
        "arn:aws:lambda:*:*:function:*:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "states:DescribeExecution",
        "states:StartExecution"
      ],
      "Resource" : [
```

```
        "arn:aws:states:*:*:stateMachine:SSM*",
        "arn:aws:states:*:*:execution:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSSMManagedEC2InstanceDefaultPolicy

`AmazonSSMManagedEC2InstanceDefaultPolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memungkinkan fungsionalitasAWS Systems Manager pada instans EC2.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSSMManagedEC2InstanceDefaultPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 Agustus 2022, 20:54 UTC
- Waktu yang telah diedit: 30 Agustus 2022, 20.54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
```

```
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSSMManagedInstanceCore

`AmazonSSMManagedInstanceCore`adalah kebijakanAWS terkelola yang: Kebijakan untuk Peran Amazon EC2 untuk mengaktifkan fungsionalitas inti layananAWS Systems Manager.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSSMManagedInstanceCore` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 15 Maret 2019 17:22 UTC
- Waktu yang telah diedit: 23 Mei 2019 16.54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
```

```
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonSSMPatchAssociation

`AmazonSSMPatchAssociation`adalah kebijakanAWS terkelola yang: Menyediakan akses ke instance turunan untuk operasi asosiasi patch.

Menggunakan kebijakan

Anda dapat melampirkan`AmazonSSMPatchAssociation` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 13 Mei 2020
- Waktu yang telah diedit: 13 Mei 2020, 16.00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMPatchAssociation`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ssm:DescribeEffectivePatchesForPatchBaseline",
      "Resource" : "arn:aws:ssm:*:*:patchbaseline/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:GetPatchBaseline",
      "Resource" : "arn:aws:ssm:*:*:patchbaseline/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:DescribePatchBaselines",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSSMReadOnlyAccess

`AmazonSSMReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Amazon SSM.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSSMReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 Mei 2015, 17:44 UTC
- Waktu yang telah diedit: 29 Mei 2015 07.44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSSMServiceRolePolicy

`AmazonSSMServiceRolePolicy`adalah kebijakanAWS terkelola yang: Menyediakan akses keAWS Sumber Daya yang dikelola atau digunakan oleh Amazon SSM

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 November 2017, 19:20 UTC
- Waktu yang telah diedit: 14 September 2022, 19.46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListTagsForResource",
        "ssm:GetCalendarState"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SSM*",
        "arn:aws:lambda:*:*:function:*:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "states:DescribeExecution",
        "states:StartExecution"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:SSM*",
        "arn:aws:states:*:*:execution:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:SelectResourceConfig"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEnrollmentStatus"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeCases"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeComplianceByResource",
        "config:DescribeRemediationConfigurations",
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarms",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:ListStackSets",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackInstances",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:DeleteStackSet"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:DeleteStackInstances",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*",
        "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-SSM*:*",
        "arn:aws:cloudformation:*:*:type/resource/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/SSMExplorerManagedRule"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "events:DescribeRule",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "securityhub:DescribeHub",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonSumerianFullAccess

`AmazonSumerianFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Sumerian.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonSumerianFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: April 24, 2018, 20:14 UTC
- Waktu yang telah diedit: 24 April 2018 08.08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSumerianFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sumerian:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonTextractFullAccess

`AmazonTextractFullAccess`adalah kebijakanAWS terkelola yang: Akses ke semua API Amazon Textract

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonTextractFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 28 November 2018, 19:07 UTC
- Waktu yang telah diedit: 28 November 2018 19.07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTextractFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "textract:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonTextractServiceRole

`AmazonTextractServiceRole`adalah kebijakanAWS terkelola yang: Memungkinkan Textract untuk memanggilAWS layanan atas nama Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonTextractServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 28 November 2018
- Waktu yang telah diedit: 28 November 2018 07.12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:AmazonTextract*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonTimestreamConsoleFullAccess

`AmazonTimestreamConsoleFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh untuk mengelola Amazon Timestream menggunakanAWS Management Console. Perhatikan bahwa kebijakan ini juga memberikan izin untuk operasi KMS tertentu, dan operasi untuk mengelola kueri yang disimpan. Jika menggunakan CMK yang dikelola Pelanggan, silakan lihat dokumentasi untuk izin tambahan yang diperlukan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonTimestreamConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 September 2020, 21:47 UTC
- Waktu yang telah diedit: 01 Pebruari 2022, 21.37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:timestream:database-name"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "timestream.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dbqms:CreateFavoriteQuery",
```

```
        "dbqms:DescribeFavoriteQueries",
        "dbqms:UpdateFavoriteQuery",
        "dbqms:DeleteFavoriteQueries",
        "dbqms:GetQueryString",
        "dbqms:CreateQueryHistory",
        "dbqms:DescribeQueryHistory",
        "dbqms:UpdateQueryHistory",
        "dbqms:DeleteQueryHistory"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonTimestreamFullAccess

`AmazonTimestreamFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Timestream. Perhatikan bahwa kebijakan ini juga memberikan akses operasi KMS

tertentu. Jika menggunakan CMK yang dikelola Pelanggan, silakan lihat dokumentasi untuk izin tambahan yang diperlukan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonTimestreamFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 September 2020, 21:47 UTC
- Waktu yang telah diedit: 26 November 2021 23.42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:timestream:database-name"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "timestream.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonTimestreamInfluxDBFullAccess

`AmazonTimestreamInfluxDBFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses administratif penuh untuk membuat, memperbarui, menghapus, dan mencantumkan instans

Amazon TimeStream InfluxDB serta membuat dan mencantumkan grup parameter. Silakan merujuk ke dokumentasi untuk izin tambahan yang diperlukan.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonTimestreamInfluxDBFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Maret 2024, 22:53 UTC
- Waktu telah diedit: 14 Maret 2024, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TimestreamInfluxDBStatement",
      "Effect" : "Allow",
      "Action" : [
        "timestream-influxdb:CreateDbParameterGroup",
        "timestream-influxdb:GetDbParameterGroup",
        "timestream-influxdb:ListDbParameterGroups",
        "timestream-influxdb:CreateDbInstance",
        "timestream-influxdb:DeleteDbInstance",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:TagResource",
```

```
        "timestream-influxdb:UntagResource",
        "timestream-influxdb:ListTagsForResource",
        "timestream-influxdb:UpdateDbInstance"
      ],
      "Resource" : [
        "arn:aws:timestream-influxdb:*:*:*"
      ]
    },
    {
      "Sid" : "ServiceLinkedRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/timestream-
influxdb.amazonaws.com/AWSServiceRoleForTimestreamInfluxDB",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "timestream-influxdb.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BucketValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonTimestreamInfluxDBServiceRolePolicy

`AmazonTimestreamInfluxDBServiceRolePolicy`adalah kebijakan AWS terkelola yang: Menyediakan akses administratif penuh untuk membuat, memperbarui, menghapus, dan mencantumkan instans Amazon TimeStream InfluxDB serta membuat dan mencantumkan grup parameter. Silakan merujuk ke dokumentasi untuk izin tambahan yang diperlukan.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 Maret 2024, 18:53 UTC
- Waktu telah diedit: 14 Maret 2024, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
```

```
      ]
    },
    {
      "Sid" : "CreateEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonTimestreamInfluxDBManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CreateTagWithEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonTimestreamInfluxDBManaged" : "false"
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "ManageEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonTimestreamInfluxDBManaged" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "PutCloudWatchMetricsStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Timestream/InfluxDB",
            "AWS/Usage"
          ]
        }
      },
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ManageSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:READONLY-InfluxDB-auth-parameters-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonTimestreamReadOnlyAccess

`AmazonTimestreamReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Amazon Timestream. Kebijakan juga memberikan izin untuk membatalkan kueri yang sedang berjalan. Jika menggunakan CMK yang dikelola Pelanggan, silakan lihat dokumentasi untuk izin tambahan yang diperlukan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonTimestreamReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 September 2020, 21:47 UTC
- Waktu yang telah diedit: 28 Februari 2023, 18.22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:CancelQuery",
```

```
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:Select",
        "timestream:SelectValues",
        "timestream:DescribeScheduledQuery",
        "timestream:ListScheduledQueries",
        "timestream:DescribeBatchLoadTask",
        "timestream:ListBatchLoadTasks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonTranscribeFullAccess

`AmazonTranscribeFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke operasi Amazon Transcribe

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonTranscribeFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 04 April 2018, 16:06 UTC
- Waktu yang telah diedit: 04 April 2018 16.06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*transcribe*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonTranscribeReadOnlyAccess

`AmazonTranscribeReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses ke operasi baca saja untuk Amazon Transcribe

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonTranscribeReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: April 04, 2018, 16:05 UTC
- Waktu yang telah diedit: 04 April 2018 16.05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:Get*",
```

```
        "transcribe:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonVPCCrossAccountNetworkInterfaceOperations

`AmazonVPCCrossAccountNetworkInterfaceOperations`adalah kebijakan AWS terkelola yang: Menyediakan akses untuk membuat antarmuka jaringan dan melampirkannya ke sumber daya lintas akun

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVPCCrossAccountNetworkInterfaceOperations` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 Juli 2017, 20:47 UTC
- Waktu yang telah diedit: September 25, 2023, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:ReplaceRoute"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonVPCFullAccess

`AmazonVPCFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke Amazon VPC melalui. AWS Management Console

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVPCFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 08 Februari 2024, 16:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCFullAccess`

Versi kebijakan

Versi kebijakan: v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachClassicLinkVpc",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCarrierGateway",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
```

```
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateFlowLogs",
        "ec2:CreateInternetGateway",
        "ec2:CreateLocalGatewayRouteTableVpcAssociation",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpointConnectionNotification",
        "ec2:CreateVpcEndpointServiceConfiguration",
        "ec2:CreateVpcPeeringConnection",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteCarrierGateway",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteEgressOnlyInternetGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteLocalGatewayRouteTableVpcAssociation",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpcEndpointConnectionNotifications",
        "ec2:DeleteVpcEndpointServiceConfigurations",
```

```
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
```

```
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DetachClassicLinkVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLink",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVpcClassicLink",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySecurityGroupRules",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ModifyVpcEndpointConnectionNotification",
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:ModifyVpcPeeringConnectionOptions",
        "ec2:ModifyVpcTenancy",
        "ec2:MoveAddressToVpc",
        "ec2:RejectVpcEndpointConnections",
        "ec2:RejectVpcPeeringConnection",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:ResetNetworkInterfaceAttribute",
        "ec2:RestoreAddressToClassic",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

`AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`adalah kebijakan AWS terkelola yang: Menyediakan izin untuk mendeskripsikan AWS sumber daya, menjalankan Network Access Analyzer, dan membuat atau menghapus tag pada Network Insights Access Scope dan Network Insights Access Scope Analysis.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVPCNetworkAccessAnalyzerFullAccessPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Juni 2023, 22:56 UTC
- Waktu telah diedit: November 03, 2023, 19:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsAccessScope",
        "ec2:DeleteNetworkInsightsAccessScope",
        "ec2:DeleteNetworkInsightsAccessScopeAnalysis",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
```

```
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAccessScopeAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-insights-access-scope/*",
        "arn:*:ec2:*:*:network-insights-access-scope-analysis/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tiros:CreateQuery",
```

```
        "tiros:GetQueryAnswer"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonVPCReachabilityAnalyzerFullAccessPolicy

`AmazonVPCReachabilityAnalyzerFullAccessPolicy`adalah kebijakan AWS terkelola yang: Menyediakan izin untuk mendeskripsikan AWS sumber daya, menjalankan Reachability Analyzer, dan membuat atau menghapus tag di Jalur Wawasan Jaringan dan Analisis Wawasan Jaringan.

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVPCReachabilityAnalyzerFullAccessPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 Juni 2023, 20:12 UTC
- Waktu telah diedit: November 03, 2023, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerFullAccessPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
```

```
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-insights-path/*",
        "arn:*:ec2:*:*:network-insights-analysis/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

`AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini dilampirkan pada peran IAMRoleForReachabilityAnalyzerCrossAccountResource Access. Peran ini diterapkan ke akun anggota dalam organisasi ketika akun manajemen memungkinkan akses tepercaya untuk Reachability Analyzer. Ini memberikan izin untuk melihat sumber daya dari seluruh organisasi Anda menggunakan konsol Reachability Analyzer.

Menggunakan Kebijakan ini

Anda dapat melampirkan`AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Mei 2023, 20:38 UTC
- Waktu yang telah diedit: 01 Mei 2023, 20.38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:Describe*",
        "network-firewall:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonVPCReadOnlyAccess

`AmazonVPCReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya baca ke Amazon VPC melalui. AWS Management Console

Menggunakan kebijakan ini

Anda dapat melampirkan `AmazonVPCReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu telah diedit: 08 Februari 2024, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
```

```
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AmazonWorkDocsFullAccess

`AmazonWorkDocsFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon WorkDocs melaluiAWS Management Console

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonWorkDocsFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 16 April 2020, 23:05 UTC

- Waktu yang telah diedit: 16 April 2020, 23.05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonWorkDocsReadOnlyAccess

`AmazonWorkDocsReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Amazon WorkDocs melaluiAWS Management Console

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonWorkDocsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 Januari 2020, 23:49 UTC
- Waktu yang telah diedit: 08 Januari 2020 23.49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonWorkMailEventsServiceRolePolicy

`AmazonWorkMailEventsServiceRolePolicy`adalah kebijakanAWS terkelola yang: Mengaktifkan akses keLayanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon WorkMail Events

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

detail kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 16 April 2019, 16:52 UTC
- Waktu yang telah diedit: 16 April 2019 16.52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan

kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

JSON kebijakan JSON kebijakan JSON kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonWorkMailFullAccess

`AmazonWorkMailFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke WorkMail, Directory Service, SES, EC2 dan akses baca ke metadata KMS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonWorkMailFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC

- Waktu yang telah diedit: 21 Desember 2020, 14.13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailFullAccess`

Versi kebijakan

Versi kebijakan:v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:CheckAlias",
        "ds:CreateAlias",
        "ds:CreateDirectory",
        "ds:CreateIdentityPoolDirectory",
        "ds:DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:ListAuthorizedApplications",
        "ds:UnauthorizeApplication",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "route53:ChangeResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53:GetHostedZone",
        "route53domains:CheckDomainAvailability",
        "route53domains:ListDomains",
        "ses:*",
        "workmail:*",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "events.workmail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.workmail.amazonaws.com/
AWSServiceRoleForAmazonWorkMailEvents*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : "arn:aws:iam::*:role/*workmail*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "events.workmail.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonWorkMailMessageFlowFullAccess

`AmazonWorkMailMessageFlowFullAccess`adalah kebijakanAWS terkelola yang: Akses penuh ke API Alur WorkMail Pesan

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonWorkMailMessageFlowFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Februari 2021, 11:08 UTC
- Waktu yang telah diedit: 11 Februari 2021 11.08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workmailmessageflow:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonWorkMailMessageFlowReadOnlyAccess

`AmazonWorkMailMessageFlowReadOnlyAccess`adalah kebijakanAWS terkelola yang: Hanya membaca akses ke WorkMail pesan untuk GetRawMessageContent API

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonWorkMailMessageFlowReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 28 Januari 2021, 12:40 UTC
- Waktu yang telah diedit: 28 Januari 2021 08.40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "workmailmessageflow:Get*"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonWorkMailReadOnlyAccess

`AmazonWorkMailReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke WorkMail dan SES.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonWorkMailReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 25 Juli 2019, 08:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:Describe*",
        "ses:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "lambda:ListFunctions",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonWorkSpacesAdmin

`AmazonWorkSpacesAdmin`adalahAWSkebijakan terkelolabahwa: Menyediakan akses ke AmazonWorkSpacestindakan administratif melaluiAWSSDK dan CLI.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonWorkSpacesAdmin`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 22 September 2015, 22:21 UTC
- Waktu yang diedit:03 Agustus 2023, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin`

Versi kebijakan

Versi kebijakan: v5(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys",
        "workspaces:CreateTags",
        "workspaces:CreateWorkspaceImage",
        "workspaces:CreateWorkspaces",
        "workspaces:CreateStandbyWorkspaces",
        "workspaces:DeleteTags",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspacesConnectionStatus",
        "workspaces:ModifyCertificateBasedAuthProperties",
        "workspaces:ModifySamlProperties",
        "workspaces:ModifyWorkspaceProperties",
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:RestoreWorkspace",
        "workspaces:StartWorkspaces",
        "workspaces:StopWorkspaces",
        "workspaces:TerminateWorkspaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM

- Memulai denganAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonWorkSpacesApplicationManagerAdminAccess

`AmazonWorkSpacesApplicationManagerAdminAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses administrator untuk mengemas aplikasi di Amazon WorkSpaces Application Manager.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonWorkSpacesApplicationManagerAdminAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 April 2015, 14:03 UTC
- Waktu yang telah diedit: 09 April 2015 14.03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wam:AuthenticatePackager",
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonWorkspacesPCAAccess

`AmazonWorkspacesPCAAccess`adalah kebijakanAWS terkelola yang: Kebijakan terkelola ini menyediakan akses administratif penuh ke sumber daya CA PribadiAWS Certificate Manager di otentikasi berbasis sertifikat AndaAkun AWS.

Menggunakan kebijakan

Anda dapat melampirkan`AmazonWorkspacesPCAAccess` ke pengguna, grup, dan peran Anda.

detail

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 November 2022, 00:25 UTC
- Waktu yang telah diedit: 08 November 2022, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:*:acm-pca:*:*:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/euc-private-ca" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonWorkSpacesSelfServiceAccess

`AmazonWorkSpacesSelfServiceAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses ke layanan WorkSpaces backend Amazon untuk melakukan tindakan Workspace Self Service

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonWorkSpacesSelfServiceAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Juni 2019, 19:22 UTC
- Waktu yang telah diedit: 27 Juni 2019, 19.22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:ModifyWorkspaceProperties"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonWorkSpacesServiceAccess

`AmazonWorkSpacesServiceAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses akun pelanggan keAWS WorkSpaces layanan untuk meluncurkan Workspace.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonWorkSpacesServiceAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Juni 2019, 19:19 UTC
- Waktu yang telah diedit: 18 Maret 2020, 23.32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AmazonWorkSpacesWebReadOnly

`AmazonWorkSpacesWebReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke Amazon WorkSpaces Web dan dependensinya melaluiAWS Management Console, SDK, dan CLI.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonWorkSpacesWebReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 November 2021, 14:20 UTC
- Waktu yang telah diedit: 02 November 2022, 20.20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserSettings",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserSettings",
        "workspaces-web:ListUserAccessLoggingSettings"
      ],
      "Resource" : "arn:aws:workspaces-web:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonWorkSpacesWebServiceRolePolicy

`AmazonWorkSpacesWebServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan akses keLayanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon WorkSpaces Web

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 November 2021, 13:15 UTC
- Waktu yang telah diedit: 15 Desember 2022, 22.46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan default adalah versi yang menentukan izin untuk kebijakan default. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/WorkSpacesWebManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "WorkSpacesWebManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/WorkSpacesWebManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/WorkSpacesWeb",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStreamSummary"
      ],
```

```
      "Resource" : "arn:aws:kinesis:*:*:stream/amazon-workspaces-web-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonZocaloFullAccess

`AmazonZocaloFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Zocalo.

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonZocaloFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 18.41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:*",
        "ds:*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmazonZocaloReadOnlyAccess

`AmazonZocaloReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Amazon Zocalo

Menggunakan kebijakan ini

Anda dapat melampirkan`AmazonZocaloReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 18.41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AmplifyBackendDeployFullAccess

`AmplifyBackendDeployFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan izin akses penuh Amplify untuk menerapkan sumber daya backend Amplify (, Amazon AWS AppSync Cognito, Amazon S3, dan layanan terkait lainnya) melalui Kit Pengembangan (CDK) AWS Cloud AWS

Menggunakan kebijakan ini

Anda dapat melampirkan `AmplifyBackendDeployFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Oktober 2023, 21:32 UTC
- Waktu telah diedit: 02 Januari 2024, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CDKPreDeploy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplateSummary"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/amplify-*",
        "arn:aws:cloudformation:*:*:stack/CDKToolkit/*"
      ]
    },
    {
      "Sid" : "AmplifyMetadata",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "cloudformation:ListStacks",
        "ssm:DescribeParameters",
        "appsync:GetIntrospectionSchema",
        "amplify:GetBackendEnvironment"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableResources",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetSchemaCreationStatus",
        "appsync:StartSchemaCreation",
        "appsync:UpdateResolver",
        "appsync:ListFunctions",
        "appsync:UpdateFunction",
        "appsync:UpdateApiKey"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableSchemaResource",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:amplify-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifySchema",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*amplify*",
        "arn:aws:s3:::cdk-*-assets-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CDKDeploy",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cdk-*-deploy-role-*-*",
        "arn:aws:iam::*:role/cdk-*-file-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-image-publishing-role-*-*",
```

```
        "arn:aws:iam::*:role/cdk-*-lookup-role-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath",
        "ssm:GetParameters",
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amplify/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyModifySSMParam",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:DeleteParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

APIGatewayServiceRolePolicy

`APIGatewayServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan API Gateway untuk mengelolaAWS Sumber Daya terkait atas nama pelanggan.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 Oktober 2017, 17:23 UTC
- Waktu yang telah diedit: 12 Juli 2021 22.24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v9 (default)

Versi standar kebijakan ini adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/amazon-apigateway-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:GetCertificate"
```

```
      ],
      "Resource" : "arn:aws:acm:*:*:certificate/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Owner",
            "VpcLinkId"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "servicediscovery:GetNamespace",
```

```
      "Resource" : "arn:aws:servicediscovery:*:*:namespace/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "servicediscovery:GetService",
      "Resource" : "arn:aws:servicediscovery:*:*:service/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AppIntegrationsServiceLinkedRolePolicy

`AppIntegrationsServiceLinkedRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan AppIntegrations untuk mengelola AppFlow sumber daya dan mempublikasikan data CloudWatch metrik atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna,, atau peran.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 September 2022, 19:42 UTC
- Waktu yang telah diedit: 30 September 2022, 19.42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AppIntegrations"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeConnectorEntity",
        "appflow:ListConnectorEntities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeConnectorProfiles",
        "appflow:UseConnectorProfile"
      ],
      "Resource" : "arn:aws:appflow:*:*:connector-profile/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DeleteFlow",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
```

```
        "appflow:StartFlow",
        "appflow:StopFlow",
        "appflow:UpdateFlow"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AppIntegrationsManaged" : "true"
        }
      },
      "Resource" : "arn:aws:appflow:*:*:flow/FlowCreatedByAppIntegrations-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:TagResource"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AppIntegrationsManaged"
          ]
        }
      },
      "Resource" : "arn:aws:appflow:*:*:flow/FlowCreatedByAppIntegrations-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ApplicationAutoScalingForAmazonAppStreamAccess

`ApplicationAutoScalingForAmazonAppStreamAccess`adalah kebijakanAWS terkelola yang: Kebijakan untuk mengaktifkan Penskalaan Otomatis Aplikasi untuk Amazon AppStream

Menggunakan kebijakan ini

Anda dapat melampirkan`ApplicationAutoScalingForAmazonAppStreamAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2017, 21:39 UTC
- Waktu yang telah diedit: 06 Februari 2017 21.39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
```

```
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

`ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan akses keLayanan AWS dan Sumber Daya yang digunakan atau dikelola oleh fitur Ekspor Berkelanjutan Application Discovery Service

Menggunakan kebijakan

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 09 Agustus 2018, 20:22 UTC
- Waktu yang telah diedit: 13 Agustus 2018 02.31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:UpdateTable",
        "firehose:CreateDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "logs:CreateLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "firehose:DeleteDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:UpdateDestination"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
    },
    {
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::aws-application-discovery-service*"
    },
```

```
    {
      "Action" : [
        "s3:GetObject"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::aws-application-discovery-service*/*"
    },
    {
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutRetentionPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "firehose.amazonaws.com"
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "firehose.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AppRunnerNetworkingServiceRolePolicy

`AppRunnerNetworkingServiceRolePolicy`adalah kebijakanAWS terkelola yang: MemungkinkanAWS AppRunner Jaringan untuk mengelolaAWS sumber daya terkait atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Januari 2022, 21:02 UTC
- Waktu yang telah diedit: 12 Januari 2022, 21.02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AWSAppRunnerManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "StringLike" : {
          "aws:RequestTag/AWSAppRunnerManaged" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSAppRunnerManaged" : "false"
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AppRunnerServiceRolePolicy

`AppRunnerServiceRolePolicy`adalah kebijakanAWS terkelola yang: MemungkinkanAWS AppRunner untuk mengelolaAWS sumber daya terkait atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda dapat melampirkan kebijakan ini pada pengguna, grup, atau peran tidak dapat dilampirkan pada pengguna, grup, grup, grup, atau peran peran peran

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 Mei 2021, 19:15 UTC
- Waktu yang telah diedit: 14 Mei 2021 07.15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/apprunner/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/apprunner/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AWSAppRunnerManagedRule*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AutoScalingConsoleFullAccess

`AutoScalingConsoleFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Auto Scaling melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AutoScalingConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 12 Januari 2017, 19:43 UTC
- Waktu yang telah diedit: 06 Pebruari 2018 08.08 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
```

```
        "ec2:CreateKeyPair",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:ImportKeyPair"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListSubscriptions",
        "sns:ListTopics"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menentukan dan menghapus dan menghapus dan
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AutoScalingConsoleReadOnlyAccess

`AutoScalingConsoleReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke Auto Scaling melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AutoScalingConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 12 Januari 2017 19.48 UTC
- Waktu yang telah diedit: 12 Januari 2017 19.48 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
```

```
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListSubscriptions",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AutoScalingFullAccess

`AutoScalingFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Auto Scaling.

Menggunakan kebijakan ini

Anda dapat melampirkan`AutoScalingFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 12 Januari 2017, 19:31 UTC

- Waktu yang telah diedit: 06 Februari 2018 09.59 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricAlarm",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcClassicLink"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AutoScalingNotificationAccessRole

`AutoScalingNotificationAccessRole`adalah kebijakanAWS terkelola yang: Kebijakan default untuk peran layanan Akses AutoScaling Pemberitahuan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AutoScalingNotificationAccessRole` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 18.41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AutoScalingReadOnlyAccess

`AutoScalingReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke Auto Scaling.

Menggunakan kebijakan ini

Anda dapat melampirkan`AutoScalingReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 12 Januari 2017 19.39 UTC
- Waktu yang telah diedit: 12 Januari 2017 19.39 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus menghapus menghapus identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AutoScalingServiceRolePolicy

`AutoScalingServiceRolePolicy`adalah kebijakan AWS terkelola yang: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Auto Scaling

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 08 Januari 2018, 23:10 UTC
- Waktu telah diedit: 29 Februari 2024, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachClassicLinkVpc",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateFleet",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:DetachClassicLinkVpc",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2InstanceProfileManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "EC2SpotManagement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ELBManagement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Register*",
        "elasticloadbalancing:Deregister*",
        "elasticloadbalancing:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWManagement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSManagement",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridgeRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
```

```
        "events:PutTargets",
        "events:RemoveTargets",
        "events:DeleteRule",
        "events:DescribeRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemsManagerParameterManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpcLatticeManagement",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:DeregisterTargets",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListTargets",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWS_ConfigRole

`AWS_ConfigRole`adalah kebijakan AWS terkelola yang: Kebijakan default untuk AWS peran layanan Config. Menyediakan izin yang diperlukan untuk AWS Config untuk melacak perubahan pada sumber daya Anda AWS .

Menggunakan kebijakan ini

Anda dapat melampirkan `AWS_ConfigRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 15 September 2020, 20:30 UTC
- Waktu yang telah diedit: 22 Februari 2024, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWS_ConfigRole`

Versi kebijakan

Versi kebijakan: v30 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigRoleStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
```

```
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListThemes",
        "apigateway:GET",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListEventIntegrationAssociations",
        "app-integrations:ListEventIntegrations",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "appmesh:DescribeGatewayRoute",
```

```
        "appmesh:DescribeMesh",
        "appmesh:DescribeRoute",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApiCache",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "APS:DescribeRuleGroupsNamespace",
        "APS:DescribeWorkspace",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListTagsForResource",
        "APS:ListWorkspaces",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:ListAssessments",
```

```
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
```

```
        "cassandra:Select",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListTypes",
        "cloudfront:GetFunction",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:ListDistributions",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeRepository",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetReportGroups",
```

```
        "codebuild:ListReportGroups",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codedeploy:GetDeploymentConfig",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelines",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config:Select*",
        "connect:DescribeEvaluationForm",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribePhoneNumber",
        "connect:DescribePrompt",
```

```
        "connect:DescribeQuickConnect",
        "connect:DescribeRule",
        "connect:DescribeUser",
        "connect:GetTaskTemplate",
        "connect:ListApprovedOrigins",
        "connect:ListEvaluationForms",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPrompts",
        "connect:ListQuickConnects",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListUsers",
        "connect:SearchAvailablePhoneNumbers",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
```

```
        "datasync:ListLocations",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "detective:ListGraphs",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "dms:DescribeCertificates",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:DescribeClientVpnAuthorizationRules",
```

```
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeFleets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAddon",
        "eks:DescribeCluster",
```

```
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:ListAddons",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
```

```
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "finspace:GetEnvironment",
```

```
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:ListPolicies",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "forecast:ListTagsForResource",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
```

```
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
```

```
        "glue:GetPartitions",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetWorkflow",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:ListComponents",
        "greengrass:ListComponentVersions",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
```

```
        "guardduty:ListThreatIntelSets",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADevices",
        "iam:ListMFADeviceTags",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "imagebuilder:GetComponent",
```

```
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:ListAuthorizers",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
```

```
        "iot:ListMitigationActions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
```

```
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
```

```
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:ListConnectors",
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
```

```
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDistributions",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:GetDataProtectionPolicy",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
```

```
        "lookoutmetrics:ListTagsForResource",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListTagsForResource",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeFlow",
        "mediaconnect:ListFlows",
        "mediaconnect:ListTagsForResource",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListPlaybackConfigurations",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "mobiletargeting:GetApp",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaign",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetEmailChannel",
        "mobiletargeting:GetEmailTemplate",
```

```
        "mobiletargeting:GetEventStream",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:GetSegment",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTagsForResource",
        "mobiletargeting:ListTemplates",
        "mq:DescribeBroker",
        "mq:ListBrokers",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "opsworks:DescribeInstances",
        "opsworks:DescribeLayers",
        "opsworks:DescribeTimeBasedAutoScaling",
        "opsworks:DescribeVolumes",
        "opsworks:ListTags",
        "organizations:DescribeAccount",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
```

```
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
```

```
        "quicksight:ListAnalyses",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
```

```
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListServices",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListTagsForResource",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "robomaker:DescribeRobotApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListRobotApplications",
        "robomaker:ListSimulationApplications",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
```

```
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:GetChange",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListQueryLoggingConfigs",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver:ListTagsForResource",
        "rum:GetAppMonitor",
```

```
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
```

```
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3express:GetBucketPolicy",
        "s3express:ListAllMyDirectoryBuckets",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeWorkteam",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
```

```
        "sagemaker:ListPipelines",
        "sagemaker:ListProjects",
        "sagemaker:ListTags",
        "sagemaker:ListWorkteams",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "sdb:GetAttributes",
        "sdb:ListDomains",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:DescribeHub",
        "serviceCatalog:DescribePortfolioShares",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetEmailTemplate",
        "ses:GetTemplate",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListEmailTemplates",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListTemplates",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeSubscription",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "sns:GetDataProtectionPolicy",
```

```
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetDocument",
        "ssm:ListDocuments",
        "ssm:ListTagsForResource",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:ListActivities",
        "states:ListStateMachines",
        "states:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
```

```
        "tag:GetResources",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConfigLogStreamStatementID",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "ConfigLogEventsStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAccountActivityAccess

`AWSAccountActivityAccess`adalah kebijakanAWS terkelola yang: Memungkinkan pengguna mengakses halaman Aktivitas Akun.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSAccountActivityAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 07 Maret 2023, 17.02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountActivityAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetChallengeQuestions",
        "account:GetContactInformation",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "payments:ListPaymentPreferences"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus izin identitas identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSAccountManagementFullAccess

`AWSAccountManagementFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke ManajemenAWS Akun.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSAccountManagementFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 September 2021, 23:20 UTC
- Waktu yang telah diedit: 30 September 2021 02.20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "account:*",
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSAccountManagementReadOnlyAccess

`AWSAccountManagementReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke ManajemenAWS Akun

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSAccountManagementReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 September 2021, 23:29 UTC
- Waktu yang telah diedit: 30 September 2021 02.29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan kebijakan adalah versi default kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:Get*",
        "account:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSAccountUsageReportAccess

`AWSAccountUsageReportAccess`adalah kebijakanAWS terkelola yang: Memungkinkan pengguna mengakses halaman Laporan Penggunaan Akun.

Menggunakan kebijakan

Anda dapat melampirkan`AWSAccountUsageReportAccess` ke pengguna, grup, dan peran Anda.

detail

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 18.41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountUsageReportAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewUsage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSAgentlessDiscoveryService

`AWSAgentlessDiscoveryService`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk Discovery Agentless Connector untuk mendaftar denganAWS Application Discovery Service.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSAgentlessDiscoveryService` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 02 Agustus 2016, 01:35 UTC
- Waktu yang telah diedit: 24 Februari 2020, 23.08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "awsconnector:RegisterConnector",
        "awsconnector:GetConnectorHealth"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::connector-platform-upgrade-info/*",
        "arn:aws:s3:::connector-platform-upgrade-info",
        "arn:aws:s3:::connector-platform-upgrade-bundles/*",
        "arn:aws:s3:::connector-platform-upgrade-bundles",
        "arn:aws:s3:::connector-platform-release-notes/*",
        "arn:aws:s3:::connector-platform-release-notes",
        "arn:aws:s3:::prod.agentless.discovery.connector.upgrade/*",
        "arn:aws:s3:::prod.agentless.discovery.connector.upgrade"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::import-to-ec2-connector-debug-logs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    },
    {
      "Sid" : "Discovery",
      "Effect" : "Allow",
      "Action" : [
        "Discovery:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "arsenal",
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSAppFabricFullAccess

`AWSAppFabricFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke AWS AppFabric layanan dan hanya membaca akses ke layanan dependen seperti S3, Kinesis, KMS.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppFabricFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2023, 19:51 UTC
- Waktu yang telah diedit: 27 Juni 2023, 19.51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appfabric:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSListAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FirehoseReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowUseOfServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "appfabric.amazonaws.com"
        }
      },
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appfabric.amazonaws.com/
AWSServiceRoleForAppFabric"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSAppFabricReadOnlyAccess

`AWSAppFabricReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya baca ke AWS AppFabric

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSAppFabricReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2023, 19:52 UTC
- Waktu yang telah diedit: 27 Juni 2023, 19.52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appfabric:GetAppAuthorization",
        "appfabric:GetAppBundle",
        "appfabric:GetIngestion",
        "appfabric:GetIngestionDestination",
        "appfabric:ListAppAuthorizations",
        "appfabric:ListAppBundles",
        "appfabric:ListIngestionDestinations",
        "appfabric:ListIngestions",
        "appfabric:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSAppFabricServiceRolePolicy

`AWSAppFabricServiceRolePolicy`adalah kebijakan AWS terkelola yang: Menyediakan AppFabric akses ke AWS sumber daya atas nama Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 Juni 2023, 21:07 UTC
- Waktu yang telah diedit: 26 Juni 2023, 21.07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEmitMetric",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AppFabric"
        }
      }
    },
    {
      "Sid" : "S3PutObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*/AWSAppFabric/*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FirehosePutRecord",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/AWSAppFabricManaged" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationAutoscalingAppStreamFleetPolicy

`AWSApplicationAutoscalingAppStreamFleetPolicy`adalah kebijakanAWS terkelola yang: Kebijakan pemberian izin untuk Application Auto Scaling untuk mengakses AppStream dan CloudWatch.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 Oktober 2017, 19:04 UTC
- Waktu yang telah diedit: 20 Oktober 2017 19.04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang mengizinkan untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
```

```
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSApplicationAutoscalingCassandraTablePolicy

`AWSApplicationAutoscalingCassandraTablePolicy`adalah kebijakanAWS terkelola yang: Kebijakan pemberian izin untuk Application Auto Scaling untuk mengakses Cassandra dan CloudWatch.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 Maret 2020, 22:49 UTC
- Waktu yang telah diedit: 18 Maret 2020 22.49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cassandra:Select",
      "Resource" : [
        "arn:*:cassandra:*:*:/keyspace/system/table/*",
        "arn:*:cassandra:*:*:/keyspace/system_schema/table/*",
        "arn:*:cassandra:*:*:/keyspace/system_schema_mcs/table/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Alter",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSApplicationAutoscalingComprehendEndpointPolicy

`AWSApplicationAutoscalingComprehendEndpointPolicy`adalah kebijakanAWS terkelola yang: Kebijakan pemberian izin untuk Application Auto Scaling untuk mengakses Comprehend dan CloudWatch.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 November 2019, 18:39 UTC
- Waktu yang telah diedit: 14 November 2019 18.39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi standar kebijakan ini adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
```

```
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationAutoScalingCustomResourcePolicy

`AWSApplicationAutoScalingCustomResourcePolicy`adalah kebijakanAWS terkelola yang: Kebijakan yang memberikan izin untuk Application Auto Scaling untuk mengakses ApigateWay dan CloudWatch untuk penskalaan sumber daya khusus

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 04 Juni 2018, 23:22 UTC
- Waktu yang telah diedit: 04 Juni 2018 08.08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Kebijakan ini adalah versi yang menentukan izin untuk kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationAutoscalingDynamoDBTablePolicy

`AWSApplicationAutoscalingDynamoDBTablePolicy`adalah kebijakanAWS terkelola yang: Kebijakan yang memberikan izin untuk Application Auto Scaling untuk mengakses DynamoDB dan CloudWatch.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 Oktober 2017, 21:34 UTC
- Waktu yang telah diedit: 20 Oktober 2017 21.34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

`AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`adalah kebijakanAWS terkelola yang: Kebijakan pemberian izin untuk Application Auto Scaling untuk mengakses EC2 Spot Fleet dan CloudWatch.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 25 Oktober 2017, 18:23 UTC
- Waktu yang telah diedit: 25 Oktober 2017 06.23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
```

```
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationAutoscalingECSServicePolicy

`AWSApplicationAutoscalingECSServicePolicy`adalah kebijakanAWS terkelola yang: Kebijakan pemberian izin untuk Application Auto Scaling untuk mengakses EC2 Container Service dan CloudWatch.

Menggunakan kebijakan ini terkelak kebijakan ini.

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

detail kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 25 Oktober 2017, 23:53 UTC
- Waktu yang telah diedit: 25 Oktober 2017 23.53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan kebijakan kebijakan ini adalah versi yang menentukan izin kebijakan ini. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationAutoscalingElastiCacheRGPolicy

`AWSApplicationAutoscalingElastiCacheRGPolicy`adalah kebijakanAWS terkelola yang: Kebijakan yang memberikan izin kepada Application Auto Scaling untuk mengakses Amazon ElastiCache dan Amazon CloudWatch.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran baru.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 Agustus 2021, 23:41 UTC
- Waktu yang telah diedit: 17 Agustus 2021 23.41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticache:DescribeReplicationGroups",
        "elasticache:ModifyReplicationGroupShardConfiguration",
        "elasticache:IncreaseReplicaCount",
        "elasticache:DecreaseReplicaCount",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameters",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationAutoscalingEMRInstanceGroupPolicy

`AWSApplicationAutoscalingEMRInstanceGroupPolicy`adalah kebijakanAWS terkelola yang: Kebijakan pemberian izin untuk Application Auto Scaling untuk mengakses Elastic Map Reduce dan CloudWatch.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, grup, grup, grup, grup, grup, grup, grup, grup, grup, atau peran baru

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 Oktober 2017, 00:57 UTC
- Waktu yang telah diedit: 26 Oktober 2017 08.57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationAutoscalingKafkaClusterPolicy

`AWSApplicationAutoscalingKafkaClusterPolicy`adalah kebijakanAWS terkelola yang: Kebijakan pemberian izin untuk Application Auto Scaling untuk mengakses Managed Streaming for Apache Kafka dan CloudWatch.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 Agustus 2020
- Waktu yang telah diedit: 24 Agustus 2020 18.36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan default. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSApplicationAutoscalingLambdaConcurrencyPolicy

`AWSApplicationAutoscalingLambdaConcurrencyPolicy`adalah kebijakanAWS terkelola yang: Kebijakan yang memberikan izin kepada Application Auto Scaling untuk mengakses Lambda dan CloudWatch.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Oktober 2019, 20:04 UTC
- Waktu yang telah diedit: 21 Oktober 2019 20.04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Kebijakan ini adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationAutoscalingNeptuneClusterPolicy

`AWSApplicationAutoscalingNeptuneClusterPolicy`adalah kebijakanAWS terkelola yang: Kebijakan yang memberikan izin kepada Application Auto Scaling untuk mengakses Amazon Neptune dan Amazon CloudWatch.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 02 September 2021, 21:14 UTC
- Waktu yang telah diedit: 02 September 2021 21.14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterParameters",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "rds:AddTagsToResource",
      "Resource" : [
        "arn:aws:rds:*:*:db:autoscaled-reader*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : "neptune"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "rds:CreateDBInstance",
      "Resource" : [
        "arn:aws:rds:*:*:db:autoscaled-reader*",
        "arn:aws:rds:*:*:cluster:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : "neptune"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:autoscaled-reader*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationAutoscalingRDSClusterPolicy

`AWSApplicationAutoscalingRDSClusterPolicy`adalah kebijakanAWS terkelola yang: Kebijakan pemberian izin untuk Application Auto Scaling untuk mengakses RDS dan CloudWatch.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 Oktober 2017, 17:46 UTC
- Waktu yang telah diedit: 07 Agustus 2018 07.14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CreateDBInstance",
        "rds:DeleteDBInstance",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "rds:ModifyDBCluster",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "rds.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationAutoscalingSageMakerEndpointPolicy

`AWSApplicationAutoscalingSageMakerEndpointPolicy`adalah kebijakan AWS terkelola yang: Kebijakan yang memberikan izin ke Application Auto Scaling untuk mengakses dan. SageMaker CloudWatch

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 06 Februari 2018, 19:58 UTC
- Waktu telah diedit: 13 November 2023, 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMaker",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SageMakerCloudWatchUpdate",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationDiscoveryAgentAccess

`AWSApplicationDiscoveryAgentAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses bagi Agen Penemuan untuk mendaftar keAWS Application Discovery Service.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSApplicationDiscoveryAgentAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Mei 2016, 21:38 UTC
- Waktu yang telah diedit: 24 Februari 2020, 22.26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationDiscoveryAgentlessCollectorAccess

`AWSApplicationDiscoveryAgentlessCollectorAccess`adalah kebijakanAWS terkelola yang: Memungkinkan Pengumpul Tanpa Agen Application Discovery Service untuk memperbarui, mendaftar, dan berkomunikasi secara auto dengan Application Discovery Service

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSApplicationDiscoveryAgentlessCollectorAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 16 Agustus 2022, 21:00 UTC
- Waktu yang telah diedit: 16 Agustus 2022, 21.00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentlessCollectorAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:DescribeImages"
      ],
      "Resource" : "arn:aws:ecr-
public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sts:GetServiceBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSApplicationDiscoveryServiceFullAccess

`AWSApplicationDiscoveryServiceFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh untuk melihat dan menandai Item Konfigurasi yang dikelola olehAWS Application Discovery Service

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSApplicationDiscoveryServiceFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Mei 2016, 21:30 UTC
- Waktu yang telah diedit: 19 Juni 2019, 21.21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:*",
        "discovery:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
```

```
    {
      "Action" : [
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "continuousexport.discovery.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "migrationhub.amazonaws.com",
            "dmsintegration.migrationhub.amazonaws.com",
            "smsintegration.migrationhub.amazonaws.com"
          ]
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationMigrationAgentInstallationPolicy

`AWSApplicationMigrationAgentInstallationPolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memungkinkan pemasangan AgenAWS Replikasi, yang digunakan denganAWS Application Migration Service (MGN) untuk memigrasi server eksternal keAWS. Lampirkan kebijakan ini kepada pengguna IAM Anda atau peran yang kredensialnya Anda berikan saat menginstal AgenAWS Replikasi.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSApplicationMigrationAgentInstallationPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 19 Juni 2022, 07:51 UTC
- Waktu yang telah diedit: 20 September 2022, 11:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:RegisterAgentForMgn",
        "mgn:VerifyClientRoleForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:IssueClientCertificateForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "mgn:CreateAction" : "RegisterAgentForMgn"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationMigrationAgentPolicy

`AWSApplicationMigrationAgentPolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memungkinkan pemasangan dan penggunaan AgenAWS Replikasi, yang digunakan denganAWS Application Migration Service (MGN) untuk memigrasi server eksternal keAWS. Lampirkan kebijakan ini kepada pengguna IAM Anda atau peran yang kredensialnya Anda berikan saat menginstal AgenAWS Replikasi.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSApplicationMigrationAgentPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 07 April 2021, 07:00 UTC
- Waktu yang telah diedit: 20 September 2022, 11:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan kebijakan default adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:RegisterAgentForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationMigrationAgentPolicy_v2

`AWSApplicationMigrationAgentPolicy_v2`adalah kebijakanAWS terkelola yang: Kebijakan ini memungkinkan penggunaan AgenAWS Replikasi, yang digunakan denganAWS Application Migration Service (MGN) untuk memigrasi server eksternal keAWS. Kami tidak menyarankan Anda melampirkan kebijakan ini kepada pengguna atau peran IAM.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSApplicationMigrationAgentPolicy_v2` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Juni 2022, 14:14 UTC
- Waktu yang telah diedit: 06 Juni 2022, 14.14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn",
        "mgn:IssueClientCertificateForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/${aws:SourceIdentity}"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSApplicationMigrationConversionServerPolicy

`AWSApplicationMigrationConversionServerPolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memungkinkan Server Konversi Layanan Migrasi Aplikasi (MGN), yang merupakan instans EC2 yang diluncurkan oleh Layanan Migrasi Aplikasi, untuk berkomunikasi dengan layanan MGN. Peran IAM dengan kebijakan ini dilampirkan (sebagai Profil Instans EC2) oleh MGN ke Server Konversi MGN, yang secara otomatis diluncurkan dan diakhiri oleh MGN, bila diperlukan. Kami tidak menyarankan Anda melampirkan kebijakan ini untuk pengguna IAM. Server Konversi MGN digunakan oleh Layanan Migrasi Aplikasi saat pengguna memilih untuk meluncurkan instance Uji atau Cutover menggunakan konsol MGN, CLI, atau API.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSApplicationMigrationConversionServerPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 April 2021, 06:48 UTC
- Waktu yang telah diedit: 07 April 2021 06.48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationMigrationEC2Access

`AWSApplicationMigrationEC2Access`adalah kebijakanAWS terkelola yang: Kebijakan ini menyediakan operasi Amazon EC2 yang diperlukan untuk menggunakan Application Migration Service (MGN) untuk meluncurkan server yang dimigrasi sebagai instans EC2. Lampirkan kebijakan ini ke pengguna atau peran IAM Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSApplicationMigrationEC2Access` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 07 April 2021, 07:05 UTC
- Waktu yang telah diedit: 06 Pebruari 2023, 16.07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
```

```
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
```

```
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
```

```
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
```

```
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        },
        "Bool" : {
```

```
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:ModifyVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationMigrationFullAccess

`AWSApplicationMigrationFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin untuk semua API publik Layanan MigrasiAWS Aplikasi (MGN), serta izin untuk membaca informasi kunci KMS. Lampirkan kebijakan ini ke pengguna atau peran IAM Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSApplicationMigrationFullAccess` ke pengguna, grup, dan peran Anda.

Rincian Kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 07 April 2021, 06:56 UTC
- Waktu yang telah diedit: 20 April 2023, 17.28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess`

Versi kebijakan

Versi kebijakan:v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeKeyPairs",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListInstanceProfiles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole",
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithDrsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommandInvocations"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "drs:DisconnectSourceServer"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceConfiguredDR" : "false"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-definition/AWSMigration-*:$DEFAULT",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "mgn.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:ListCommands",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSApplicationMigrationMGHAccess

`AWSApplicationMigrationMGHAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memungkinkanAWS Application Migration Service (MGN) untuk mengirim meta-data tentang

kemajuan server yang dimigrasi menggunakan MGN toAWS Migration Hub (MGH). MGN secara otomatis membuat peran IAM dengan kebijakan ini terlampir, dan mengambil peran ini. Kami tidak menyarankan Anda melampirkan kebijakan ini kepada pengguna IAM atau peran.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSApplicationMigrationMGHAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 April 2021, 07:10 UTC
- Waktu yang telah diedit: 07 April 2021 07.10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
```

```
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSApplicationMigrationReadOnlyAccess

`AWSApplicationMigrationReadOnlyAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin untuk semua API publik hanya-baca dari Application Migration Service (MGN), serta beberapa API hanya-baca dariAWS layanan lain yang diperlukan untuk membuat penggunaan konsol MGN hanya-baca penuh. Lampirkan kebijakan ini ke pengguna atau peran IAM Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSApplicationMigrationReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 07 April 2021, 07:15 UTC
- Waktu yang telah diedit: 20 Maret 2023, 08:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:DescribeJobLogItems",
        "mgn:DescribeJobs",
        "mgn:DescribeSourceServers",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:GetLaunchConfiguration",
        "mgn:DescribeVcenterClients",
        "mgn:GetReplicationConfiguration",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:ListSourceServerActions",
        "mgn:ListTemplateActions",
        "mgn:ListApplications",
        "mgn:ListWaves",
        "mgn:ListExports",
        "mgn:ListImports",
        "mgn:ListImportErrors",
        "mgn:ListExportErrors"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationMigrationReplicationServerPolicy

`AWSApplicationMigrationReplicationServerPolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memungkinkan Server Replikasi Layanan Migrasi Aplikasi (MGN), yang merupakan instans EC2 yang diluncurkan oleh Layanan Migrasi Aplikasi - untuk berkomunikasi dengan layanan MGN, dan untuk membuat snapshot EBS di AndaAkun AWS. Peran IAM dengan kebijakan ini dilampirkan (sebagai Profil Instans EC2) oleh Layanan Migrasi Aplikasi ke Server Replikasi MGN yang secara otomatis diluncurkan dan diakhiri oleh MGN, sesuai kebutuhan. Server Replikasi MGN digunakan untuk memfasilitasi replikasi data dari server eksternal AndaAWS, sebagai bagian dari proses migrasi yang dikelola menggunakan MGN. Kami tidak menyarankan Anda melampirkan kebijakan ini kepada pengguna IAM Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSApplicationMigrationReplicationServerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 April 2021, 07:21 UTC
- Waktu yang telah diedit: 07 April 2021 07.21 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn",
        "mgn:GetAgentSnapshotCreditsForMgn",
        "mgn:DescribeReplicationServerAssociationsForMgn",
        "mgn:DescribeSnapshotRequestsForMgn",
        "mgn:BatchDeleteSnapshotRequestForMgn",
        "mgn:NotifyAgentAuthenticationForMgn",
        "mgn:BatchCreateVolumeSnapshotGroupForMgn",
        "mgn:UpdateAgentReplicationProcessStateForMgn",
        "mgn:NotifyAgentReplicationProgressForMgn",
        "mgn:NotifyAgentConnectedForMgn",
        "mgn:NotifyAgentDisconnectedForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationMigrationServiceEc2InstancePolicy

`AWSApplicationMigrationServiceEc2InstancePolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini memungkinkan penginstalan dan penggunaan Agen AWS Replikasi, yang digunakan oleh AWS Application Migration Service (AWSMGN) untuk memigrasikan server sumber yang berjalan di EC2 (Cross-region atau Cross-AZ). Peran IAM dengan kebijakan ini harus dilampirkan (sebagai Profil Instans EC2) ke Instans EC2.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSApplicationMigrationServiceEc2InstancePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 22 Agustus 2023, 13:19 UTC
- Waktu telah diedit: 03 Januari 2024, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "MgnAgentInstallation",
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientLogsForMgn",
        "mgn:RegisterAgentForMgn",
        "mgn:GetAgentInstallationAssetsForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MgnAgentReplication",
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    },
    {
      "Sid" : "MgnSourceServerTagResource",
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "mgn:CreateAction" : "RegisterAgentForMgn"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSApplicationMigrationServiceRolePolicy

`AWSApplicationMigrationServiceRolePolicy`adalah kebijakan AWS terkelola yang: Memungkinkan Layanan Migrasi AWS aplikasi untuk membuat dan mengelola AWS sumber daya atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 April 2021, 06:43 UTC
- Waktu yang telah diedit: 20 Juni 2023, 09:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgn:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVolumes",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : "arn:aws:organizations::*:account/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage",
        "ec2:DeregisterImage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
```

```
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
```

```
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationReplicationServerRole",
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances"
          ]
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationMigrationSSMAccess

`AWSApplicationMigrationSSMAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini menyediakan akses ke operasi Amazon SSM yang diperlukan untuk menggunakan Application Migration Service (MGN) untuk menjalankan dokumen SSM perintah posting migrasi kustom. Lampirkan kebijakan ini ke pengguna atau peran IAM Anda.

Menggunakan kebijakan

Anda dapat melampirkan`AWSApplicationMigrationSSMAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 November 2022, 09:29 UTC
- Waktu yang telah diedit: 20 Maret 2023, 10.57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocumentVersions",
        "ssm:GetDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSApplicationMigrationVCenterClientPolicy

`AWSApplicationMigrationVCenterClientPolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memungkinkan menginstal dan menggunakan KlienAWS vCenter, yang digunakan denganAWS Application Migration Service (MGN) untuk memigrasi server eksternal keAWS. Lampirkan kebijakan ini untuk pengguna IAM Anda atau peran yang kredensialnya Anda berikan saat menginstal KlienAWS vCenter.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSApplicationMigrationVCenterClientPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 November 2021, 12:53 UTC
- Waktu yang telah diedit: 08 November 2021 12.53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:CreateVcenterClientForMgn",
        "mgn:DescribeVcenterClients"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetVcenterClientCommandsForMgn",
        "mgn:SendVcenterClientCommandResultForMgn",
        "mgn:SendVcenterClientLogsForMgn",
        "mgn:SendVcenterClientMetricsForMgn",
        "mgn:DeleteVcenterClient",
        "mgn:TagResource",
        "mgn:NotifyVcenterClientStartedForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:vcenter-client/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSAppMeshEnvoyAccess

`AWSAppMeshEnvoyAccess`adalah kebijakanAWS terkelola yang: Kebijakan Utusan App Mesh untuk mengakses konfigurasi Node Virtual.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSAppMeshEnvoyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 Juli 2019, 21:29 UTC

- Waktu yang telah diedit: 03 Juli 2019, 21.29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh:StreamAggregatedResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSAppMeshFullAccess

`AWSAppMeshFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS App Mesh API dan Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSAppMeshFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 16 April 2019, 17:50 UTC
- Waktu yang telah diedit: 07 Januari 2021 19.54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshFullAccess`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appmesh.amazonaws.com/
AWSServiceRoleForAppMesh",
      "Condition" : {
```

```
        "StringLike" : {
          "iam:AWSServiceName" : [
            "appmesh.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStack*",
        "cloudformation:UpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSAppMesh-GettingStarted-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "acm:DescribeCertificate",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSAppMeshPreviewEnvoyAccess

`AWSAppMeshPreviewEnvoyAccess`adalah kebijakanAWS terkelola yang: Kebijakan Utusan App Mesh Preview untuk mengakses konfigurasi Node Virtual.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSAppMeshPreviewEnvoyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 05 Agustus 2019, 23:32 UTC
- Waktu yang telah diedit: 05 Agustus 2019 23.32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh-preview:StreamAggregatedResources"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSAppMeshPreviewServiceRolePolicy

`AWSAppMeshPreviewServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan akses keLayanan AWS dan Sumber Daya yang digunakan atau dikelola olehAWS App Mesh

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, grup, grup, grup, grup, grup, grup, grup, kebijakan ini tidak dapat dilampirkan

detail kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 Juni 2019, 19:07 UTC
- Waktu yang telah diedit: 21 Agustus 2019 21.06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan Ketika

pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JJSON JSON JSON JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSAppMeshReadOnly

`AWSAppMeshReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca keAWS App Mesh API dan Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSAppMeshReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 16 April 2019, 17:51 UTC
- Waktu yang telah diedit: 07 Januari 2021 19.53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshReadOnly`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh:Describe*",
        "appmesh:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSAppMesh-GettingStarted-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "acm:DescribeCertificate",
```

```
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSAppMeshServiceRolePolicy

`AWSAppMeshServiceRolePolicy`adalah kebijakan AWS terkelola yang: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh AWS AppMesh

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 03 Juni 2019, 18:30 UTC

- Waktu telah diedit: 10 Oktober 2023, 16:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAppRunnerFullAccess

`AWSAppRunnerFullAccess`adalah kebijakanAWS terkelola yang: Memberikan izin untuk semua tindakan App Runner.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSAppRunnerFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Januari 2022, 04:02 UTC
- Waktu yang telah diedit: 11 Januari 2022, 04:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/apprunner.amazonaws.com/
AWSServiceRoleForAppRunner",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "apprunner.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "apprunner.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRunnerAdminAccess",
      "Effect" : "Allow",
      "Action" : "apprunner:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSAppRunnerReadOnlyAccess

`AWSAppRunnerReadOnlyAccess`adalah kebijakanAWS terkelola yang: Memberikan izin untuk mencantumkan dan melihat detail tentang sumber daya App Runner.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSAppRunnerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Februari 2022, 21:24 UTC

- Waktu yang telah diedit: 24 Februari 2022, 21.24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apprunner:List*",
        "apprunner:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSAppRunnerServicePolicyForECRAccess

`AWSAppRunnerServicePolicyForECRAccess`adalah kebijakanAWS terkelola yang: Kebijakan layananAWS App Runner yang memberikan izin baca ke sumber daya Amazon ECR di akun

pelanggan. Gunakan dalam peran yang diteruskan ke App Runner saat membuat atau memperbarui layanan App Runner.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSAppRunnerServicePolicyForECRAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Mei 2021, 19:17 UTC
- Waktu yang telah diedit: 14 Mei 2021 07.17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSAppSyncAdministrator

`AWSAppSyncAdministrator`adalah kebijakanAWS terkelola yang: Menyediakan akses administratif ke AppSync layanan, meskipun tidak cukup untuk mengakses melalui konsol.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSAppSyncAdministrator` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 20 Maret 2018, 21:20 UTC
- Waktu yang telah diedit: 04 November 2019, 19.23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncAdministrator`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "appsync.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "appsync.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appsync.amazonaws.com/
AWSServiceRoleForAppSync*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSAppSyncInvokeFullAccess

`AWSAppSyncInvokeFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke AppSync layanan - baik melalui konsol maupun secara mandiri

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSAppSyncInvokeFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 20 Maret 2018, 21:21 UTC
- Waktu yang telah diedit: 20 Maret 2018, 21.21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSAppSyncPushToCloudWatchLogs

`AWSAppSyncPushToCloudWatchLogs`adalah kebijakanAWS terkelola yang: Memungkinkan AppSync untuk mendorong log ke CloudWatch akun pengguna.

Menggunakan kebijakan

Anda dapat melampirkan`AWSAppSyncPushToCloudWatchLogs` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 09 April 2018, 19:38 UTC
- Waktu yang telah diedit: 09 April 2018 07.38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSAppSyncSchemaAuthor

`AWSAppSyncSchemaAuthor`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk membuat, memperbarui, dan query skema.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSAppSyncSchemaAuthor` ke pengguna, grup, dan peran Anda.

Detail

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 20 Maret 2018, 21:21 UTC
- Waktu yang telah diedit: 01 Pebruari 2023, 18.36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:CreateResolver",
        "appsync:CreateType",
        "appsync:DeleteResolver",
        "appsync:DeleteType",
        "appsync:GetResolver",
        "appsync:GetType",
```

```
        "appsync:GetDataSource",
        "appsync:GetSchemaCreationStatus",
        "appsync:GetIntrospectionSchema",
        "appsync:GetGraphqlApi",
        "appsync:ListTypes",
        "appsync:ListApiKeys",
        "appsync:ListResolvers",
        "appsync:ListDataSources",
        "appsync:ListGraphqlApis",
        "appsync:StartSchemaCreation",
        "appsync:UpdateResolver",
        "appsync:UpdateType",
        "appsync:TagResource",
        "appsync:UntagResource",
        "appsync:ListTagsForResource",
        "appsync:CreateFunction",
        "appsync:UpdateFunction",
        "appsync:GetFunction",
        "appsync:DeleteFunction",
        "appsync:ListFunctions",
        "appsync:ListResolversByFunction",
        "appsync:EvaluateMappingTemplate",
        "appsync:EvaluateCode"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSAppSyncServiceRolePolicy

`AWSAppSyncServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan akses keAWS layanan dan sumber daya yang digunakan atau dikelola oleh AppSync

Menggunakan kebijakan ini terkait kebijakan ini.

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Kebijakan ini tidak dapat melampirkan kebijakan ini ke pengguna Anda.

detail kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Januari 2020, 19:56 UTC
- Waktu yang telah diedit: 21 Januari 2020 19.56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan kebijakan kebijakan JSON JSON JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSArtifactAccountSync

`AWSArtifactAccountSync`adalah kebijakanAWS terkelola yang: Memungkinkan akses hanya-bacaAWS Artifact ke operasi diAWS Organizations.

Menggunakan kebijakan

Anda dapat melampirkan`AWSArtifactAccountSync` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: April 10, 2018, 23:04 UTC
- Waktu yang telah diedit: 10 April 2018 03.05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSArtifactReportsReadOnlyAccess

`AWSArtifactReportsReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya-baca ke laporan layanan AWS Artifact.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSArtifactReportsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Januari 2024, 22:42 UTC
- Waktu telah diedit: 02 Januari 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSArtifactServiceRolePolicy

`AWSArtifactServiceRolePolicy`adalah sebuah[AWSkebijakan terkelola](#)itu: MemungkinkanAWSArtefak untuk mengumpulkan informasi tentang organisasi melaluiAWSLayanan organisasi.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Agustus 2023, 20:27 UTC
- Waktu yang diedit:21 Agustus 2023, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1(default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber dayaAWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
```

```
        "organizations:DescribeAccount",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- MemulaidenganAWSkebijakan terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAuditManagerAdministratorAccess

`AWSAuditManagerAdministratorAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses administratif untuk mengaktifkan atau menonaktifkanAWS Audit Manager, memperbarui pengaturan, dan mengelola penilaian, kontrol, dan kerangka kerja

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSAuditManagerAdministratorAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Desember 2020, 20:02 UTC
- Waktu yang telah diedit: 30 April 2022, 00.02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AuditManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "auditmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOnlyAuditManagerIntegration",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "auditmanager.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "IAMAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMAccessCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "auditmanager.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMAccessManageSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:UpdateRoleDescription",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*"
    },
    {
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "auditmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SNSAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "ForAllValues:StringEquals" : {
```

```
          "events:source" : [
            "aws.securityhub"
          ]
        }
      }
    },
    {
      "Sid" : "EventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
    },
    {
      "Sid" : "TagAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSAuditManagerServiceRolePolicy

`AWSAuditManagerServiceRolePolicy`adalah kebijakan AWS terkelola yang: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh AWS Audit Manager

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 08 Desember 2020, 15:12 UTC
- Waktu telah diedit: 06 Desember 2023, 20:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "backup:ListRecoveryPointsByResource",
        "bedrock:GetCustomModel",
```

```
        "bedrock:GetFoundationModel",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListCustomModels",
        "bedrock:ListFoundationModels",
        "bedrock:ListModelCustomizationJobs",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cognito-idp:DescribeUserPool",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:ListDiscoveredResources",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "dynamodb:DescribeTable",
        "dynamodb:ListBackups",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetEbsDefaultKmsKeyId",
```

```
        "ec2:GetEbsEncryptionByDefault",
        "ecs:DescribeClusters",
        "eks:DescribeAddonVersions",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeServiceUpdates",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeSslPolicies",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListSecurityConfigurations",
        "events:DescribeRule",
        "events:ListConnections",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRules",
        "firehose:ListDeliveryStreams",
        "fsx:DescribeFileSystems",
        "guardduty:ListDetectors",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListOpenIdConnectProviders",
        "iam:ListPolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSamlProviders",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "kafka:ListClusters",
        "kafka:ListKafkaVersions",
        "kinesis:ListStreams",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
```

```
        "kms:ListKeys",
        "lambda:ListFunctions",
        "license-manager:ListAssociationsForLicenseConfiguration",
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListUsageForLicenseConfiguration",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:FilterLogEvents",
        "organizations:DescribeOrganization",
        "organizations:DescribePolicy",
        "rds:DescribeCertificates",
        "rds:DescribeDbClusterEndpoints",
        "rds:DescribeDbClusterParameterGroups",
        "rds:DescribeDbClusters",
        "rds:DescribeDBInstances",
        "rds:DescribeDbSecurityGroups",
        "redshift:DescribeClusters",
        "route53:GetQueryLoggingConfig",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketVersioning",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:ListAllMyBuckets",
        "securityhub:DescribeStandards",
        "sns:ListTopics",
        "sqs:ListQueues",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:ListRuleGroups",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListWebACLs",
        "waf:ListActivatedRulesInRuleGroup"
      ],
      "Resource" : "*",
      "Sid" : "AuditManagerAPICallAccess"
    },
    {
      "Sid" : "AuditManagerS3GetBucketPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
      "Condition" : {
        "StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "Null" : {
          "events:source" : "false"
        },
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.securityhub"
          ]
        }
      }
    },
    {
      "Sid" : "EventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSAutoScalingPlansEC2AutoScalingPolicy

`AWSAutoScalingPlansEC2AutoScalingPolicy`adalah kebijakanAWS terkelola yang: Kebijakan yang memberikan izin kepadaAWS Auto Scaling untuk memperkirakan kapasitas secara berkala dan menghasilkan tindakan penskalaan terjadwal untuk grup Auto Scaling dalam rencana penskalaan

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 Agustus 2018, 22:46 UTC
- Waktu yang telah diedit: 23 Agustus 2018 02.46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSBackupAuditAccess

`AWSBackupAuditAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin bagi pengguna untuk membuat kontrol dan kerangka kerja yang menentukan harapan mereka untukAWS Mencadangkan sumber daya dan aktivitas, serta untuk mengaudit Sumber daya dan aktivitasAWS Backup terhadap kontrol dan kerangka kerja yang ditentukan. Kebijakan ini memberikan izin kepadaAWS Config dan layanan serupa untuk menjelaskan harapan pengguna melakukan audit. Kebijakan ini juga memberikan izin untuk menyampaikan laporan audit ke S3 dan layanan serupa, dan memungkinkan pengguna untuk menemukan dan membuka laporan audit mereka.

Menggunakan kebijakan

Anda dapat melampirkan`AWSBackupAuditAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Agustus 2021, 01:02 UTC
- Waktu yang telah diedit: 10 April 2023, 21.23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAuditAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateFramework",
        "backup:UpdateFramework",
        "backup:ListFrameworks",
        "backup:DescribeFramework",
        "backup:DeleteFramework",
        "backup:ListBackupPlans",
        "backup:ListBackupVaults",
        "backup:CreateReportPlan",
        "backup:UpdateReportPlan",
        "backup:ListReportPlans",
        "backup:DescribeReportPlan",
        "backup:DeleteReportPlan",
        "backup:StartReportJob",
        "backup:ListReportJobs",
        "backup:DescribeReportJob"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeComplianceByConfigRule"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:GetComplianceDetailsByConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSBackupDataTransferAccess

`AWSBackupDataTransferAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memungkinkan agenAWS Backint untuk menyelesaikan transfer data cadangan dengan pesawat

PenyimpananAWS Backup. Lampirkan kebijakan ini ke peran yang diasumsikan oleh Instans EC2 yang menjalankan SAP HANA dengan agen Backint.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSBackupDataTransferAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 10 November 2022, 22:48 UTC
- Waktu yang telah diedit: 10 November 2022, 22.48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupDataTransferAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:StartObject",
        "backup-storage:PutChunk",
        "backup-storage:GetChunk",
        "backup-storage:ListChunks",
        "backup-storage:ListObjects",
        "backup-storage:GetObjectMetadata",
        "backup-storage:NotifyObjectComplete"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSBackupFullAccess

`AWSBackupFullAccess`adalah kebijakan AWS terkelola yang: Kebijakan ini ditujukan untuk administrator cadangan, memberikan akses penuh ke operasi AWS Pencadangan, termasuk membuat atau mengedit rencana cadangan, menetapkan AWS sumber daya ke rencana cadangan, menghapus cadangan, dan memulihkan cadangan.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 November 2019, 22:21 UTC
- Waktu telah diedit: November 27, 2023, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupFullAccess`

Versi kebijakan

Versi kebijakan: v17 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AwsBackupStorageAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup-storage:*",
      "Resource" : "*"
    },
    {
      "Sid" : "RdsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusters",
        "rds:describeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RdsDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBSnapshot",
        "rds:DeleteDBClusterSnapshot"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DynamoDbPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListBackups",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDbDeleteBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DeleteBackup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EfsFileSystemPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFilesystems"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "Ec2Permissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:describeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2DeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:DeregisterImage"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ResourceGroupTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "StorageGatewayVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListGateways"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "StorageGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListVolumes",
        "storagegateway:ListLocalDisks"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "IamRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackup*",
        "arn:aws:iam::*:role/*AWSBackup*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "backup.amazonaws.com",
            "restore-testing.backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AwsOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:backup:backup-vault"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "backup.*.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "SystemManagerCommandPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SystemManagerSendCommandPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:DescribeBackups",
        "fsx:DescribeVolumes",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DeleteBackup",
      "Resource" : "arn:aws:fsx:*:*:backup/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "DirectoryServicePermissions",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "IamCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "backup.amazonaws.com",
            "restore-testing.backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "BackupGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:AssociateGatewayToServer",
        "backup-gateway:CreateGateway",
        "backup-gateway:DeleteGateway",
        "backup-gateway:DeleteHypervisor",
        "backup-gateway:DisassociateGatewayFromServer",
        "backup-gateway:ImportHypervisorConfiguration",
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup-gateway:PutMaintenanceStartTime",
        "backup-gateway:TagResource",
        "backup-gateway:TestHypervisorConfiguration",
        "backup-gateway:UntagResource",
        "backup-gateway:UpdateGatewayInformation",
        "backup-gateway:UpdateHypervisor"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupGatewayHypervisorPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings",
        "backup-gateway:PutHypervisorPropertyMappings",
        "backup-gateway:StartVirtualMachinesMetadataSync"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "BackupGatewayVirtualMachinePermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetVirtualMachine"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "BackupGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway",
        "backup-gateway:PutBandwidthRateLimitSchedule"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
    },
    {
      "Sid" : "CloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListTables",
        "timestream:ListDatabases"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
```

```
    {
      "Sid" : "TimestreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "RedshiftResourcesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeSnapshotSchedules"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:subnetgroup:*",
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:snapshotschedule:*"
      ]
    },
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeNodeConfigurationOptions",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterTracks"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CloudFormationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "SystemsManagerForSapPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceAccessManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

`AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`adalah kebijakanAWS terkelola yang: MemberikanAWS BackupGateway izin untuk menyinkronkan metadata Mesin Virtual atas nama Anda

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 15 Desember 2022, 19:43 UTC
- Waktu yang telah diedit: 15 Desember 2022, 19.43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListVmTags",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListTagsForResource"
      ],
```

```
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "VMTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:TagResource",
        "backup-gateway:UntagResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSBackupOperatorAccess

`AWSBackupOperatorAccess`adalah sebuahAWSkebijakan terkelolabahwa: Kebijakan ini memberikan izin kepada pengguna untuk menetapkanAWSsumber daya untuk membuat cadangan rencana, membuat cadangan sesuai permintaan, dan memulihkan cadangan. Kebijakan ini tidak mengizinkan pengguna untuk membuat atau mengedit rencana cadangan atau menghapus cadangan terjadwal setelah dibuat.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSBackupOperatorAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Tipe:AWSkebijakan terkelola
- Waktu pembuatan: 18 November 2019, 22:23 UTC

- Waktu yang diedit:September 06, 2023, 20:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOperatorAccess`

Versi kebijakan

Versi kebijakan: v15(default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber dayaAWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
        "backup:Describe*",
        "backup:CreateBackupSelection",
        "backup:DeleteBackupSelection",
        "backup:StartBackupJob",
        "backup:StartRestoreJob",
        "backup:StartCopyJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
```

```
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListBackups",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFilesystems"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:describeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListGateways"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListVolumes",
        "storagegateway:ListLocalDisks"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
```

```
        "arn:aws:iam::*:role/*AwsBackup*",
        "arn:aws:iam::*:role/*AWSBackup*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "fsx:DescribeFileSystems",
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "fsx:DescribeVolumes",
      "Resource" : "arn:aws:fsx:*:*:volume/*/*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "fsx:DescribeStorageVirtualMachines",
      "Resource" : "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetVirtualMachine"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListDatabases",
        "timestream:ListTables"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeSnapshotSchedules"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:subnetgroup:*",
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:snapshotschedule:*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeNodeConfigurationOptions",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterTracks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai denganAWSkebijakan terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupOrganizationAdminAccess

`AWSBackupOrganizationAdminAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini untuk administrator cadangan yang menggunakan manajemen cadangan lintas akun untuk mengelola cadangan untuk organisasi.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSBackupOrganizationAdminAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Juni 2020, 16:23 UTC
- Waktu yang telah diedit: 18 November 2022, 18.26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DisableAWSServiceAccess",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:account/*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:AttachPolicy",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:DetachPolicy",
```

```
        "organizations:DisablePolicyType",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListPolicies",
        "organizations:EnablePolicyType",
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:PolicyType" : [
            "BACKUP_POLICY"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSBackupRestoreAccessForSAPHANA

`AWSBackupRestoreAccessForSAPHANA`adalah kebijakanAWS terkelola yang: Memberikan izinAWS Pencadangan untuk memulihkan cadangan SAP HANA di Amazon EC2

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSBackupRestoreAccessForSAPHANA` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 10 November 2022, 22:43 UTC
- Waktu yang telah diedit: 10 November 2022, 22.43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
```

```
        "backup:Describe*",
        "backup:StartBackupJob",
        "backup:StartRestoreJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:BackupDatabase",
        "ssm-sap:RestoreDatabase",
        "ssm-sap:UpdateHanaBackupSettings",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSBackupServiceLinkedRolePolicyForBackup

`AWSBackupServiceLinkedRolePolicyForBackup`adalah kebijakan AWS terkelola yang: Menyediakan izin AWS Cadangan untuk membuat cadangan atas nama Anda di seluruh layanan AWS

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 02 Juni 2020, 23:08 UTC
- Waktu yang telah diedit: 15 Desember 2023, 22:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

Versi kebijakan

Versi kebijakan: v15 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EFSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
```

```
    },
    {
      "Sid" : "DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "elasticfilesystem:DescribeFileSystems",
        "dynamodb:ListTables",
        "storagegateway:ListVolumes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstances",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnapshotCopyTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Sid" : "EC2CreateBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AWSBackupManagedResource"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "EC2CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2RDSDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeImages",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBClusterSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CopyImage",
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeregisterImage",
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "RDSInstanceAndSnashotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CopyDBSnapshot",
        "rds:DeleteDBSnapshot",
        "rds:DeleteDBInstanceAutomatedBackup"
      ],
      "Resource" : "arn:aws:rds:*:*:snapshot:awsbackup:*"
    },
    {
      "Sid" : "RDSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CopyDBClusterSnapshot",
        "rds:DeleteDBClusterSnapshot"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
    },
    {
      "Sid" : "KMSDescribePermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
```

```
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "fsx.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "fsx.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CopyBackup",
        "fsx:TagResource",
        "fsx:DescribeBackups",
        "fsx:DeleteBackup"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
```

```
      "Sid" : "DynamoDBDeletePermissions",
      "Effect" : "Allow",
      "Action" : "dynamodb:DeleteBackup",
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "BackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListTagsForBackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTagsOfResource",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "EventBridgePermissions",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
```

```
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
      ]
    },
    {
      "Sid" : "EventBridgeRulesPermissions",
      "Effect" : "Allow",
      "Action" : "events:ListRules",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:UpdateHANABackupSettings"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeTable",
        "timestream:GetAwsBackupStatus",
        "timestream:GetAwsRestoreStatus"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
```

```
      "Sid" : "TimestreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftClusterSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DeleteClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "CloudformationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
```

```
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupServiceLinkedRolePolicyForBackupTest

`AWSBackupServiceLinkedRolePolicyForBackupTest`adalah kebijakanAWS terkelola yang: Memberikan izinAWS Backup untuk membuat cadangan atas nama Anda di seluruhAWS layanan

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

detail kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Mei 2020, 17:37 UTC
- Waktu yang telah diedit: 12 Mei 2020, 17.37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Effect" : "Allow",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
    },
    {
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSBackupServiceRolePolicyForBackup

`AWSBackupServiceRolePolicyForBackup`adalah kebijakan AWS terkelola yang: Menyediakan izin AWS Cadangan untuk membuat cadangan atas nama Anda di seluruh layanan AWS

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupServiceRolePolicyForBackup` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 Januari 2019, 21:01 UTC
- Waktu yang telah diedit: 15 Desember 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup`

Versi kebijakan

Versi kebijakan: v18 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:CreateBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
```

```
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeBackup",
        "dynamodb:DeleteBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "DynamoDBBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:ListTagsForResource",
        "rds:DescribeDBSnapshots",
        "rds:CreateDBSnapshot",
        "rds:CopyDBSnapshot",
        "rds:DescribeDBInstances",
        "rds:CreateDBClusterSnapshot",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshots",
        "rds:CopyDBClusterSnapshot",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*"
      ]
    },
    {
      "Sid" : "RDSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBCluster"
      ],
```

```
      "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RDSClusterBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBClusterAutomatedBackup"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster-auto-backup:*"
    },
    {
      "Sid" : "RDSBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBSnapshot",
        "rds:ModifyDBSnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:snapshot:awsbackup:*"
      ]
    },
    {
      "Sid" : "RDSClusterModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBClusterSnapshot",
        "rds:ModifyDBClusterSnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
      ]
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:CreateSnapshot",
        "storagegateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
```

```
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSTagAndDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSnapshotTierStatus"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "EC2TagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:image/*"
    },
    {
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "EBSSnapshotTierPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "BackupVaultPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeBackupVault",
        "backup:CopyIntoBackupVault"
      ],
      "Resource" : "arn:aws:backup:*:*:backup-vault:*"
    },
    {
```

```
      "Sid" : "BackupVaultCopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:CopyFromBackupVault"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "EBSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "KMSDynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "KMSDataKeyEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetResourcesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSendPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FsxBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxCreateBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:CreateBackup",
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeFileSystems",
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FsxVolumePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeVolumes",
      "Resource" : "arn:aws:fsx:*:*:volume/*"
    },
```

```
    {
      "Sid" : "FsxListTagsPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:ListTagsForResource",
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DeleteBackup",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:CopyBackup",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "DynamodbBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:StartAwsBackupJob",
        "dynamodb:ListTagsOfResource"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "BackupGatewayBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:Backup",
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
```

```
    {
      "Sid" : "CloudformationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*/*"
    },
    {
      "Sid" : "RedshiftCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateClusterSnapshot",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DeleteClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
```

```
    {
      "Sid" : "RedshiftResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:StartAwsBackupJob",
        "timestream:GetAwsBackupStatus",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListTagsForResource",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SSMSAPResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:BackupDatabase",
        "ssm-sap:UpdateHanaBackupSettings",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupServiceRolePolicyForRestores

`AWSBackupServiceRolePolicyForRestores`adalah kebijakan AWS terkelola yang: Menyediakan izin AWS Cadangan untuk melakukan pemulihan atas nama Anda di seluruh AWS layanan. Kebijakan ini mencakup izin untuk membuat dan menghapus AWS sumber daya, seperti volume EBS, instans RDS, dan sistem file EFS, yang merupakan bagian dari proses pemulihan.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBackupServiceRolePolicyForRestores` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 12 Januari 2019 00:23 UTC
- Waktu yang telah diedit: 15 Desember 2023, 22:05 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores`

Versi kebijakan

Versi kebijakan: v20 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:PutItem",
        "dynamodb:GetItem",
        "dynamodb:DeleteItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:RestoreTableFromBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "EBSPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "EC2DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSnapshotTierStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StorageGatewayVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DeleteVolume",
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes",
        "storagegateway:AddTagsToResource"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
```

```
        "storagegateway:CreateStorediSCSIVolume",
        "storagegateway:CreateCachediSCSIVolume"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "RDSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:RestoreDBInstanceFromDBSnapshot",
        "rds:DeleteDBInstance",
        "rds:AddTagsToResource",
        "rds:DescribeDBClusters",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:DeleteDBCluster",
        "rds:RestoreDBInstanceToPointInTime",
        "rds:DescribeDBClusterSnapshots",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Restore",
        "elasticfilesystem:CreateFilesystem",
        "elasticfilesystem:DescribeFilesystems",
        "elasticfilesystem:DeleteFilesystem",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
```

```
    {
      "Sid" : "KMSDescribePermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com",
            "ec2.*.amazonaws.com",
            "elasticfilesystem.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "redshift.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "EBSSnapshotBlockPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ebs:CompleteSnapshot",
        "ebs:StartSnapshot",
        "ebs:PutSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "RDSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBInstance"
      ],
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Sid" : "EC2DeleteAndRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:DeleteTags",
        "ec2:RestoreSnapshotTier"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2CreateTagsScopedPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:backup:source-resource"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "EC2RunInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TerminateInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "EC2CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateVolume"
          ]
        }
      }
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateFileSystemFromBackup"
      ],
      "Resource" : [
```

```
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*"
      ]
    },
    {
      "Sid" : "FsxTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FsxBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteFileSystem",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:file-system/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "FsxDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeVolumes"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*"
    },
    {
      "Sid" : "FsxVolumeTagPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:backup:source-resource"
          ]
        }
      }
    },
    {
      "Sid" : "FsxBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:storage-virtual-machine/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteVolume",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "DSPermissions",
```

```
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:RestoreTableFromAwsBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "GatewayRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:Restore"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "CloudformationChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:TagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:*/*/*"
    },
    {
      "Sid" : "RedshiftClusterSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:RestoreFromClusterSnapshot",
        "redshift:RestoreTableFromClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftClusterPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftTablePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeTableRestoreStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:StartAwsRestoreJob",
        "timestream:GetAwsRestoreStatus",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:ListDatabases",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBackupServiceRolePolicyForS3Backup

`AWSBackupServiceRolePolicyForS3Backup`adalah kebijakanAWS terkelola yang: Kebijakan yang berisi izin yang diperlukan untukAWS Backup untuk membuat cadangan data di bucket S3 mana pun. Ini termasuk akses baca ke semua objek S3 dan akses dekripsi untuk semua kunci KMS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSBackupServiceRolePolicyForS3Backup` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 18 Februari 2022, 17:40 UTC
- Waktu yang telah diedit: 01 September 2022, 16.52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "events:ListRules",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketTagging",
        "s3:GetInventoryConfiguration",
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:GetBucketAcl",
        "s3:PutInventoryConfiguration",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectAcl",
        "s3:GetObject",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:ListAllMyBuckets",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSBackupServiceRolePolicyForS3Restore

`AWSBackupServiceRolePolicyForS3Restore`adalah kebijakanAWS terkelola yang: Kebijakan yang berisi izin yang diperlukan untukAWS Backup untuk memulihkan cadangan S3 ke bucket. Ini termasuk izin baca/tulis untuk semua bucket S3, dan izin untuk GenerateDataKey dan DescribeKey untuk semua kunci KMS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSBackupServiceRolePolicyForS3Restore` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 18 Februari 2022, 17:39 UTC
- Waktu yang telah diedit: 07 Pebruari 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
```

```
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:PutBucketVersioning",
        "s3:PutBucketOwnershipControls",
        "s3:GetBucketOwnershipControls"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:DeleteObject",
        "s3:PutObjectVersionAcl",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging",
        "s3:GetObjectAcl",
        "s3:PutObjectAcl",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSBatchFullAccess

`AWSBatchFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh untuk sumber dayaAWS Batch.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSBatchFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Desember 2016, 19:35 UTC
- Waktu yang telah diedit: 24 Oktober 2022, 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBatchFullAccess`

Versi kebijakan

Versi kebijakan:v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "batch:*",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeImages",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ecs:DescribeClusters",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeCluster",
        "eks:ListClusters",
        "logs:Describe*",
        "logs:Get*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSBatchServiceRole",
        "arn:aws:iam::*:role/service-role/AWSBatchServiceRole",
        "arn:aws:iam::*:role/ecsInstanceRole",
        "arn:aws:iam::*:instance-profile/ecsInstanceRole",
        "arn:aws:iam::*:role/iaws-ec2-spot-fleet-role",
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-role",
```

```
        "arn:aws:iam::*:role/AWSBatchJobRole*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*Batch*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "batch.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus identitas IAM M M M M M M M M M M M M
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSBatchServiceEventTargetRole

`AWSBatchServiceEventTargetRole`adalah kebijakanAWS terkelola yang: Kebijakan untuk mengaktifkan Target CloudWatch Acara untuk Pengajuan JobAWS Batch

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSBatchServiceEventTargetRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 28 Februari 2018, 22:31 UTC

- Waktu yang telah diedit: 28 Februari 2018 10.31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "batch:SubmitJob"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSBatchServiceRole

`AWSBatchServiceRole`adalah kebijakan AWS terkelola yang: Kebijakan untuk peran layanan AWS Batch yang memungkinkan akses ke layanan terkait termasuk EC2, Autoscaling, layanan Container EC2, dan Cloudwatch Logs.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBatchServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Desember 2016, 19:36 UTC
- Waktu telah diedit: 05 Desember 2023, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole`

Versi kebijakan

Versi kebijakan: v13 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBatchPolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
```

```
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:CreateLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:RequestSpotFleet",
        "ec2:CancelSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:TerminateInstances",
        "ec2:RunInstances",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:SuspendProcesses",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:ListAccountSettings",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
        "ecs:RegisterTaskDefinition",
        "ecs:DeregisterTaskDefinition",
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:UpdateContainerAgent",
```

```
        "ecs:DeregisterContainerInstance",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "iam:GetInstanceProfile",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement2",
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
      "Resource" : [
        "arn:aws:ecs:*:*:task/*_Batch_*"
      ]
    },
    {
      "Sid" : "AWSBatchPolicyStatement3",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement4",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "spot.amazonaws.com",
```

```
            "spotfleet.amazonaws.com",
            "autoscaling.amazonaws.com",
            "ecs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement5",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBillingConductorFullAccess

`AWSBillingConductorFullAccess`adalah kebijakanAWS terkelola yang: Gunakan kebijakan AWSBillingConductorFullAccess terkelola untuk mengizinkan akses lengkap ke konsol dan APIAWS Billing Conductor (ABC). Kebijakan ini memungkinkan pengguna untuk membuat daftar, membuat, dan menghapus sumber daya ABC.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSBillingConductorFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 13 April 2022, 18:02 UTC
- Waktu yang telah diedit: 13 April 2022, 18.02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:*",
        "organizations:ListAccounts",
        "pricing:DescribeServices"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSBillingConductorReadOnlyAccess

`AWSBillingConductorReadOnlyAccess`adalah kebijakanAWS terkelola yang: Gunakan kebijakan AWSBillingConductorReadOnlyAccess terkelola untuk mengizinkan akses baca saja ke konsol dan APIAWS Billing Conductor (ABC). Kebijakan ini memberikan izin untuk melihat dan mencantumkan semua sumber daya ABC. Ini tidak termasuk kemampuan untuk membuat atau menghapus sumber daya.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSBillingConductorReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 13 April 2022, 18:02 UTC
- Waktu yang telah diedit: 13 April 2022, 18.02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:List*",
        "organizations:ListAccounts",
        "pricing:DescribeServices"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSBillingReadOnlyAccess

`AWSBillingReadOnlyAccess`adalah kebijakan AWS terkelola yang: Memungkinkan pengguna melihat tagihan di Konsol Penagihan.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSBillingReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Agustus 2020, 20:08 UTC
- Waktu telah diedit: 17 Januari 2024, 18:15 UTC

- ARN: `arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:ViewBilling",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetCredits",
        "billing:GetContractInformation",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "budgets:ViewBudget",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetCostAndUsage",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "ce:ListCostAllocationTags",
        "consolidatedbilling:ListLinkedAccounts",
        "consolidatedbilling:GetAccountBillingRole",
```

```
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:DescribeReportDefinitions",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentPreferences",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "sustainability:GetCarbonFootprintSummary",
        "tax:GetTaxRegistrationDocument",
        "tax:GetTaxInheritance",
        "tax:ListTaxRegistrations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

`AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin untuk mengontrolAWS sumber daya. Misalnya, memulai dan menghentikan instans EC2 atau RDS dengan menjalankan skripAWS Systems Manager (SSM).

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 25 Mei 2022, 19:03 UTC
- Waktu yang telah diedit: 25 Mei 2022, 19.03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan tersebut adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "rds:DescribeDBInstances",
        "rds:StartDBInstance",
        "rds:StopDBInstance"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StartRdsInstance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopRdsInstance:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSBudgetsActionsWithAWSResourceControlAccess

`AWSBudgetsActionsWithAWSResourceControlAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke TindakanAWS Anggaran termasuk menggunakan Tindakan Anggaran untuk mengontrol statusAWS sumber daya yang berjalan melaluiAWS Management Console

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSBudgetsActionsWithAWSResourceControlAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 15 Oktober 2020
- Waktu yang telah diedit: 15 Oktober 2020, 17.19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "budgets:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "budgets.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ModifyBilling",
        "ec2:DescribeInstances",
        "iam:ListGroups",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListPolicies",
        "organizations:ListRoots",
        "rds:DescribeDBInstances",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSBudgetsReadOnlyAccess

`AWSBudgetsReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke KonsolAWS Anggaran melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSBudgetsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 15 Oktober 2020, 17:18 UTC
- Waktu yang telah diedit: 15 Oktober 2020, 17.18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSBugBustFullAccess

`AWSBugBustFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan IAM ini memberi pengguna akses penuh keAWS BugBust konsol

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSBugBustFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Juni 2021, 07:03 UTC
- Waktu yang telah diedit: 22 Juli 2021 20.04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeGuruReviewerPermission",
      "Effect" : "Allow",
```

```
      "Action" : [
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeGuruProfilerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-profiler:DescribeProfilingGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "bugbust:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustSLRCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/bugbust.amazonaws.com/
AWSServiceRoleForBugBust",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "bugbust.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSBugBustPlayerAccess

`AWSBugBustPlayerAccess`adalah kebijakanAWS terkelola yang: Kebijakan IAM ini memberi pengguna akses untuk berpartisipasi dalamAWS BugBust acara

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSBugBustPlayerAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Juni 2021, 07:15 UTC
- Waktu yang telah diedit: 24 Juni 2021 07.15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustPlayerAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeGuruReviewerPermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeGuruProfilerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:DescribeProfilingGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustPlayerAccess",
      "Effect" : "Allow",
      "Action" : [
        "bugbust:ListBugs",
        "bugbust:ListProfilingGroups",
        "bugbust:JoinEvent",
        "bugbust:GetEvent",
        "bugbust:ListEvents",
        "bugbust:GetJoinEventStatus",
        "bugbust:ListEventScores",
        "bugbust:ListEventParticipants",
        "bugbust:UpdateWorkItem",
        "bugbust:ListPullRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSBugBustServiceRolePolicy

`AWSBugBustServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memberikan izinAWS BugBust untuk mengakses sumber daya atas nama Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

detail kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 Juni 2021, 06:59 UTC
- Waktu yang telah diedit: 24 Juni 2021 06.59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCertificateManagerFullAccess

`AWSCertificateManagerFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS Certificate Manager (ACM)

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCertificateManagerFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 21 Januari 2016, 17:02 UTC
- Waktu yang telah diedit: 17 Agustus 2020, 22.18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "acm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCertificateManagerPrivateCAAuditor

`AWSCertificateManagerPrivateCAAuditor`adalah kebijakanAWS terkelola yang: Memberikan akses auditor ke OtoritasAWS Sertifikat Certificate Manager Pribadi

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCertificateManagerPrivateCAAuditor` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 23 Oktober 2018, 16:51 UTC
- Waktu yang telah diedit: 17 Agustus 2020 22.54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:CreateCertificateAuthorityAuditReport",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetCertificateAuthorityCsr",
```

```
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:GetPolicy",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCertificateManagerPrivateCAFullAccess

`AWSCertificateManagerPrivateCAFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke OtoritasAWS Sertifikat Pribadi Certificate Manager

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCertificateManagerPrivateCAFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 23 Oktober 2018, 16:54 UTC

- Waktu yang telah diedit: 23 Oktober 2018 16.54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin izin kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCertificateManagerPrivateCAPrivilegedUser

`AWSCertificateManagerPrivateCAPrivilegedUser`adalah kebijakanAWS terkelola yang: Menyediakan akses pengguna sertifikat istimewa ke OtoritasAWS Sertifikat Pribadi Certificate Manager

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCertificateManagerPrivateCAPrivilegedUser` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 20 Juni 2019, 17:43 UTC
- Waktu yang telah diedit: 20 Juni 2019 07.43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/*CACertificate*/V*"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCertificateManagerPrivateCAReadOnly

`AWSCertificateManagerPrivateCAReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke OtoritasAWS Sertifikat Pribadi Certificate Manager

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCertificateManagerPrivateCAReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 23 Oktober 2018, 16:57 UTC
- Waktu yang telah diedit: 17 Agustus 2020 22.54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:ListCertificateAuthorities",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:GetPolicy",
      "acm-pca:ListPermissions",
```

```
      "acm-pca:ListTags"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCertificateManagerPrivateCAUser

`AWSCertificateManagerPrivateCAUser`adalah kebijakanAWS terkelola yang: Menyediakan akses pengguna sertifikat ke OtoritasAWS Sertifikat Pribadi Certificate Manager

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCertificateManagerPrivateCAUser` ke pengguna, grup, dan peran Anda.

detail kebijakan kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 23 Oktober 2018, 16:53 UTC
- Waktu yang telah diedit: 20 Juni 2019, 17.42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCertificateManagerReadOnly

`AWSCertificateManagerReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja keAWS Certificate Manager (ACM).

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCertificateManagerReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 21 Januari 2016, 17:07 UTC
- Waktu yang telah diedit: 15 Maret 2021 16.25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi izin kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan kebijakan kebijakan kebijakan dokumen kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:GetCertificate",
      "acm:ListTagsForCertificate",
      "acm:GetAccountConfiguration"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan izin izin izin izin izin izin izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSChatbotServiceLinkedRolePolicy

`AWSChatbotServiceLinkedRolePolicy`adalah kebijakanAWS terkelola yang: Peran Tertaut Layanan yang digunakan olehAWS Chatbot.

Menggunakan kebijakan ini kebijakan ini atau kebijakan ini.

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

detail kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 November 2019, 16:39 UTC
- Waktu yang telah diedit: 18 November 2019 16.39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan standar kebijakan default kebijakan standar kebijakan default kebijakan default kebijakan default kebijakan default kebijakan default kebijakan standar kebijakan default kebijakan standar kebijakan standar kebijakan standar kebijakan standar kebijakan standar kebijakan default kebijakan standar kebijakan standar kebijakan standar kebijakan default kebijakan standar kebijakan default kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Unsubscribe",
        "sns:Subscribe",
        "sns:ListSubscriptions"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/chatbot/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCleanRoomsFullAccess

`AWSCleanRoomsFullAccess`adalah kebijakan AWS terkelola yang: Memungkinkan akses penuh ke sumber daya Kamar AWS Bersih dan akses ke yang terkait Layanan AWS.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCleanRoomsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 Januari 2023, 16:10 UTC
- Waktu telah diedit: 21 Maret 2024, 15:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
```

```
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickQueryResultsBucketListAll",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "SetQueryResultsBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
    },
    {
      "Sid" : "WriteQueryResults",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleDisplayQueryResults",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
    },
    {
      "Sid" : "EstablishLogDeliveries",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCleanRoomsFullAccessNoQuerying

`AWSCleanRoomsFullAccessNoQuerying`adalahAWSkebijakan terkelolabahwa: Memungkinkan akses penuh keAWSSumber daya Kamar Bersih kecuali untuk kueri dalam kolaborasi dan akses ke terkaitLayanan AWS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCleanRoomsFullAccessNoQuerying`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 12 Januari 2023, 16:12 UTC
- Waktu yang diedit:31 Juli 2023, 20:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying`

Versi kebijakan

Versi kebijakan: v3(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:CreateAnalysisTemplate",
        "cleanrooms:CreateCollaboration",
        "cleanrooms:CreateConfiguredTable",
        "cleanrooms:CreateConfiguredTableAnalysisRule",
        "cleanrooms:CreateConfiguredTableAssociation",
        "cleanrooms:CreateMembership",
        "cleanrooms:DeleteAnalysisTemplate",
        "cleanrooms:DeleteCollaboration",
        "cleanrooms:DeleteConfiguredTable",
        "cleanrooms:DeleteConfiguredTableAnalysisRule",
        "cleanrooms:DeleteConfiguredTableAssociation",
        "cleanrooms:DeleteMember",
        "cleanrooms:DeleteMembership",
        "cleanrooms:GetAnalysisTemplate",
```

```
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:UpdateAnalysisTemplate",
        "cleanrooms:UpdateCollaboration",
        "cleanrooms:UpdateConfiguredTable",
        "cleanrooms:UpdateConfiguredTableAnalysisRule",
        "cleanrooms:UpdateConfiguredTableAssociation",
        "cleanrooms:UpdateMembership",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:UntagResource",
        "cleanrooms:TagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CleanRoomsNoQuerying",
      "Effect" : "Deny",
      "Action" : [
        "cleanrooms:StartProtectedQuery",
        "cleanrooms:UpdateProtectedQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
    },
    {
```

```
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EstablishLogDeliveries",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "SetupLogGroupsCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCleanRoomsMLFullAccess

`AWSCleanRoomsMLFullAccess`adalah kebijakan AWS terkelola yang: Memungkinkan akses penuh ke sumber daya AWS Clean Rooms dan akses ke sumber daya yang terkaitLayanan AWS.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCleanRoomsMLFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2023, 21:02 UTC
- Waktu telah diedit: 29 November 2023, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsMLFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cleanrooms-ml*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms-ml.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CollaborationMembershipCheck",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:ListMembers"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cleanrooms-ml.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AssociateModels",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:CreateConfiguredAudienceModelAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagAssociations",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:TagResource"
      ],
      "Resource" : "arn:aws:cleanrooms:*:*:membership/*/
configuredaudiencemodelassociation/*"
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/cleanrooms-ml*",
        "arn:aws:iam::*:role/role/cleanrooms-ml*"
      ]
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanroomsml*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ConsolePickOutputBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickS3Location",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*cleanrooms-ml*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCleanRoomsMLReadOnlyAccess

`AWSCleanRoomsMLReadOnlyAccess`adalah kebijakan AWS terkelola yang: Mengizinkan akses hanya-baca ke sumber daya AWS Clean Rooms dan akses hanya-baca ke sumber daya Kamar Bersih terkait AWS

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCleanRoomsMLReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2023, 20:55 UTC
- Waktu telah diedit: 29 November 2023, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CleanRoomsMLRead",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:Get*",
        "cleanrooms-ml:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCleanRoomsReadOnlyAccess

`AWSCleanRoomsReadOnlyAccess`adalah kebijakanAWS terkelola yang: Memungkinkan akses hanya-baca ke sumber dayaAWS Clean Rooms dan akses hanya-baca ke sumber dayaAWS Glue dan Amazon CloudWatch Logs terkait.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCleanRoomsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 12 Januari 2023, 16:10 UTC
- Waktu yang telah diedit: 12 Januari 2023, 16:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsRead",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGet*",
        "cleanrooms:Get*",
        "cleanrooms:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCloud9Administrator

`AWSCloud9Administrator`adalah kebijakan AWS terkelola yang: Menyediakan akses administrator ke AWS Cloud9.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloud9Administrator` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2017, 16:17 UTC
- Waktu telah diedit: 11 Oktober 2023, 12:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9Administrator`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:*",
        "iam:GetUser",
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloud9EnvironmentMember

`AWSCloud9EnvironmentMember`adalah kebijakan AWS terkelola yang: Menyediakan kemampuan untuk diundang ke lingkungan pengembangan AWS bersama Cloud9.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloud9EnvironmentMember` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2017, 16:18 UTC
- Waktu telah diedit: 11 Oktober 2023, 12:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:GetUserSettings",
        "cloud9:UpdateUserSettings",
        "iam:GetUser",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:DescribeEnvironmentMemberships"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
```

```
          "cloud9:UserArn" : "true",
          "cloud9:EnvironmentId" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloud9ServiceRolePolicy

`AWSCloud9ServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan Peran Tertaut Layanan untukAWS Cloud9

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, peran, peran Anda.

detail kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 November 2017, 13:44 UTC
- Waktu yang telah diedit: 17 Januari 2022, 14.06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-cloud9-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : "aws-cloud9-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
```

```
        "ec2:StopInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "aws-cloud9-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : [
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/cloud9/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSCloud9SSMAccessRole"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCloud9SSMInstanceProfile

`AWSCloud9SSMInstanceProfile`adalah kebijakanAWS terkelola yang: Kebijakan ini akan digunakan untuk melampirkan peran pada InstanceProfile yang akan memungkinkan Cloud9 untuk menggunakan SSM Session Manager untuk terhubung ke instance

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCloud9SSMInstanceProfile` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 14 Mei 2020, 11:40 UTC
- Waktu yang telah diedit: 14 Mei 2020, 11.40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCloud9User

`AWSCloud9User`adalah kebijakan AWS terkelola yang: Memberikan izin untuk membuat lingkungan pengembangan AWS Cloud9 dan mengelola lingkungan yang dimiliki.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloud9User` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2017, 16:16 UTC
- Waktu telah diedit: 11 Oktober 2023, 13:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9User`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:UpdateUserSettings",
        "cloud9:GetUserSettings",
        "iam:GetUser",
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:CreateEnvironmentEC2",
        "cloud9:CreateEnvironmentSSH"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "cloud9:OwnerArn" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloud9:GetUserPublicKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:DescribeEnvironmentMemberships"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true",
          "cloud9:EnvironmentId" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
```

```
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloudFormationFullAccess

`AWSCloudFormationFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS CloudFormation.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCloudFormationFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 26 Juli 2019, 21:50 UTC
- Waktu yang telah diedit: 26 Juli 2019, 21.50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCloudFormationReadOnlyAccess

`AWSCloudFormationReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses keAWS CloudFormation melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCloudFormationReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu yang telah diedit: 13 November 2019 07.40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:EstimateTemplateCost",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudformation:Detect*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCloudFrontLogger

`AWSCloudFrontLogger`adalah kebijakanAWS terkelola yang: Memberikan izin tulis kepada CloudFront Logger ke CloudWatch Log.

Menggunakan kebijakan ini.

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau

detail kebijakan.

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Juni 2018, 20:15 UTC
- Waktu yang telah diedit: 22 November 2019 19.33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default dari atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCloudHSMFullAccess

`AWSCloudHSMFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke semua sumber daya CloudHSM.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCloudHSMFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 18.39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudhsm:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCloudHSMReadOnlyAccess

`AWSCloudHSMReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke semua sumber daya CloudHSM.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCloudHSMReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 18.39 UTC

- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:Get*",
        "cloudhsm:List*",
        "cloudhsm:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCloudHSMRole

`AWSCloudHSMRole`adalah kebijakanAWS terkelola yang: Kebijakan default untuk peran layananAWS CloudHSM.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCloudHSMRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 18.41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCloudMapDiscoverInstanceAccess

`AWSCloudMapDiscoverInstanceAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses ke API penemuan AWS Cloud Peta.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudMapDiscoverInstanceAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2018, 00:02 UTC
- Waktu telah diedit: 20 September 2023, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloudMapFullAccess

`AWSCloudMapFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke semua tindakanAWS Cloud Peta.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCloudMapFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 28 November 2018

- Waktu yang telah diedit: 29 Juli 2020, 19.15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "servicediscovery:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCloudMapReadOnlyAccess

`AWSCloudMapReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya-baca ke semua tindakan AWS Cloud Peta.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudMapReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 23:45 UTC
- Waktu yang telah diedit: 20 September 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCloudMapRegisterInstanceAccess

`AWSCloudMapRegisterInstanceAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses tingkat pendaftar ke tindakan AWS Cloud Peta.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCloudMapRegisterInstanceAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2018, 00:04 UTC
- Waktu yang telah diedit: 20 September 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:DeregisterInstance",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin dengan hak istimewa paling sedikit

AWSCloudShellFullAccess

`AWSCloudShellFullAccess`adalah kebijakanAWS terkelola yang: Memberikan penggunaanAWS CloudShell dengan semua fitur

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCloudShellFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 15 Desember 2020, 18:07 UTC
- Waktu yang telah diedit: 15 Desember 2020 18.07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudShellFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudshell:*"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCloudTrail_FullAccess

`AWSCloudTrail_FullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS CloudTrail.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCloudTrail_FullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 Oktober 2020, 23:41 UTC
- Waktu yang telah diedit: 22 Februari 2021 10.01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns:SetTopicAttributes",
        "sns:GetTopicAttributes"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudtrail:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetUser"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateKey",
        "kms:CreateAlias",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCloudTrail_ReadOnlyAccess

`AWSCloudTrail_ReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya bacaAWS CloudTrail.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCloudTrail_ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 14 Juni 2022, 17:19 UTC
- Waktu yang telah diedit: 14 Juni 2022, 17.19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:Get*",
        "cloudtrail:Describe*",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

`AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini digunakan oleh peran terkait layanan bernama AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents. CloudWatch menggunakan peran terkait layanan ini untuk melakukan tindakan Manajer Insiden ManajerAWS Sistem saat CloudWatch alarm masuk ke status ALARM. Kebijakan ini memberikan izin untuk memulai insiden atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna grup grup grup grup grup grup grup grup grup grup grup grup grup grup grup grup grup grup grup grup grup grup grup grup

detail kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 27 April 2021, 13.30 UTC
- Waktu yang telah diedit: 27 April 2021 13.30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan ini adalah versi yang menentukan izin untuk kebijakan terkait kebijakan terkait kebijakan terkait kebijakan terkait kebijakan default kebijakan kebijakan terkait kebijakan default kebijakan kebijakan kebijakan kebijakan terkait kebijakan terkait kebijakan terkait kebijakan terkait kebijakan kebijakan kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan kebijakan JSON kebijakan kebijakan kebijakan kebijakan kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCodeArtifactAdminAccess

`AWSCodeArtifactAdminAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS CodeArtifact melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeArtifactAdminAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 16 Juni 2020, 23:53 UTC
- Waktu yang telah diedit: 16 Juni 2020, 23.53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCodeArtifactReadOnlyAccess

`AWSCodeArtifactReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya bacaAWS CodeArtifact melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeArtifactReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 25 Juni 2020, 21:23 UTC
- Waktu yang telah diedit: 25 Juni 2020, 21.23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:Describe*",
        "codeartifact:Get*",
        "codeartifact:List*",
        "codeartifact:ReadFromRepository"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCodeBuildAdminAccess

`AWSCodeBuildAdminAccess`adalahAWSkebijakan terkelolabahwa: Menyediakan akses penuh keAWS CodeBuildmelaluiAWS Management Console. Juga lampirkan AmazonS3ReadOnlyAccessuntuk menyediakan akses untuk mengunduh artefak build, dan melampirkan IAMFullAccessuntuk membuat dan mengelola peran layanan untukCodeBuild.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeBuildAdminAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 01 Desember 2016, 19:04 UTC
- Waktu yang diedit:31 Juli 2023, 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess`

Versi kebijakan

Versi kebijakan: v13(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "codecommit:ListRepositories",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "elasticfilesystem:DescribeFileSystems",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CWLDeleteLogGroupAccess",
      "Action" : [
        "logs:DeleteLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*:log-stream:*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
    },
    {
      "Sid" : "SSMStartSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "CodeStarConnectionsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:CreateConnection",
        "codestar-connections:DeleteConnection",
        "codestar-connections:UpdateConnectionInstallation",
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar-connections:ListConnections",
        "codestar-connections:ListInstallationTargets",
        "codestar-connections:ListTagsForResource",
        "codestar-connections:GetConnection",
        "codestar-connections:GetIndividualAccessToken",
        "codestar-connections:GetInstallationUrl",
        "codestar-connections:PassConnection",
        "codestar-connections:StartOAuthHandshake",
        "codestar-connections:UseConnection"
```

```
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai denganAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCodeBuildDeveloperAccess

`AWSCodeBuildDeveloperAccess`adalahAWSkebijakan terkelolabahwa:
Menyediakan akses keAWS CodeBuildmelaluiAWS Management Console, tetapi tidak memungkinkanCodeBuildadministrasi proyek. Juga lampirkan AmazonS3ReadOnlyAccessuntuk menyediakan akses untuk mengunduh artefak build.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeBuildDeveloperAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola

- Waktu pembuatan: 01 Desember 2016, 19:02 UTC
- Waktu yang diedit:31 Juli 2023, 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess`

Versi kebijakan

Versi kebijakan: v14(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:StartBuildBatch",
        "codebuild:StopBuildBatch",
        "codebuild:RetryBuild",
        "codebuild:RetryBuildBatch",
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codebuild:List*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
    },
    {
      "Sid" : "SSMStartSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
        }
```

```
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai denganAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCodeBuildReadOnlyAccess

`AWSCodeBuildReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya bacaAWS CodeBuild melaluiAWS Management Console. Juga lampirkan Amazons3ReadOnlyAccess untuk menyediakan akses untuk mengunduh artefak build.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeBuildReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Desember 2016, 19:03 UTC
- Waktu yang telah diedit: 14 September 2020 16.04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:List*",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "cloudwatch:GetMetricStatistics",
```

```
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCodeCommitFullAccess

`AWSCodeCommitFullAccess`adalahAWSkebijakan terkelolabahwa: Menyediakan akses penuh keAWS CodeCommitmelaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeCommitFullAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 09 Juli 2015, 17:02 UTC
- Waktu yang diedit:17 Juli 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitFullAccess`

Versi kebijakan

Versi kebijakan: v10(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "codecommit:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccessKeys",
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMUserSSHKeys",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMSelfManageServiceSpecificCredentials",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
```

```
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codecommit:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:AssociateRepository",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DisassociateRepository",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
```

```
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCodeCommitPowerUser

`AWSCodeCommitPowerUser`adalahAWSkebijakan terkelolabahwa: Menyediakan akses penuh keAWS CodeCommitrepositori, tetapi tidak memungkinkan penghapusan repositori.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeCommitPowerUser`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 09 Juli 2015, 17:06 UTC
- Waktu yang diedit:17 Juli 2023, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitPowerUser`

Versi kebijakan

Versi kebijakan: v15(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:AssociateApprovalRuleTemplateWithRepository",
        "codecommit:BatchAssociateApprovalRuleTemplateWithRepositories",
        "codecommit:BatchDisassociateApprovalRuleTemplateFromRepositories",
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Create*",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:Describe*",
        "codecommit:DisassociateApprovalRuleTemplateFromRepository",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:Merge*",
        "codecommit:OverridePullRequestApprovalRules",
        "codecommit:Put*",
        "codecommit:Post*",
        "codecommit:TagResource",
        "codecommit:Test*",
        "codecommit:UntagResource",
        "codecommit:Update*",
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccessKeys",
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMUserSSHKeys",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMSelfManageServiceSpecificCredentials",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
```

```
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codecommit:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:AssociateRepository",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DisassociateRepository",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCodeCommitReadOnly

`AWSCodeCommitReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya bacaAWS CodeCommit melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeCommitReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 Juli 2015, 17:05 UTC
- Waktu yang telah diedit: 18 Agustus 2021 08.18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitReadOnly`

Versi kebijakan

Versi kebijakan:v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
```

```
        "codecommit:Describe*",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:GitPull"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials",
        "iam:ListAccessKeys",
        "iam:GetSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codecommit:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerReadOnlyAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCodeDeployDeployerAccess

`AWSCodeDeployDeployerAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk mendaftar dan menyebarkan revisi.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeDeployDeployerAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 19 Mei 2015, 18:18 UTC
- Waktu yang telah diedit: 02 April 2020, 16.16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:CreateDeployment",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codedeploy:RegisterApplicationRevision"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codedeploy:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
```

```
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCodeDeployFullAccess

`AWSCodeDeployFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke CodeDeploy sumber daya.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeDeployFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 19 Mei 2015, 18:13 UTC
- Waktu yang telah diedit: 02 April 2020 08.14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "codedeploy:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codedeploy:*"
```

```
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCodeDeployReadOnlyAccess

`AWSCodeDeployReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke CodeDeploy sumber daya.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeDeployReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 19 Mei 2015, 18:21 UTC
- Waktu yang telah diedit: 02 April 2020, 16.20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codedeploy:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCodeDeployRole

`AWSCodeDeployRole`adalah sebuah[AWSkebijakan terkelola](#)bahwa: Menyediakan CodeDeploy akses layanan untuk memperluas tag dan berinteraksi dengan Auto Scaling atas nama Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeDeployRole`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran layanan
- Waktu pembuatan: 04 Mei 2015, 18:05 UTC
- Waktu yang diedit:16 Agustus 2023, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole`

Versi kebijakan

Versi kebijakan: v11(default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber dayaAWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:DeleteLifecycleHook",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:PutLifecycleHook",
        "autoscaling:RecordLifecycleActionHeartbeat",
        "autoscaling:CreateAutoScalingGroup",
```

```
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:EnableMetricsCollection",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:SuspendProcesses",
        "autoscaling:ResumeProcesses",
        "autoscaling:AttachLoadBalancers",
        "autoscaling:AttachLoadBalancerTargetGroups",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutWarmPool",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DeleteAutoScalingGroup",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:TerminateInstances",
        "tag:GetResources",
        "sns:Publish",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai denganAWSkebijakan terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodeDeployRoleForCloudFormation

`AWSCodeDeployRoleForCloudFormation`adalah kebijakanAWS terkelola yang: Menyediakan akses CodeDeploy layanan untuk memanggil fungsi Lambda atas nama Anda untuk melakukan penyebaran biru/hijau melalui CloudFormation.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeDeployRoleForCloudFormation` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Mei 2020, 17:12 UTC
- Waktu yang telah diedit: 19 Mei 2020, 17.12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
```

```
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCodeDeployRoleForECS

`AWSCodeDeployRoleForECS`Adalah kebijakanAWS terkelola yang: Menyediakan akses luas CodeDeploy layanan untuk melakukan penyebaran biru/hijau ECS atas nama Anda. Memberikan akses penuh ke layanan dukungan, seperti akses penuh untuk membaca semua objek S3, memanggil semua fungsi Lambda, mempublikasikan ke semua topik SNS dalam akun dan memperbarui semua layanan ECS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeDeployRoleForECS` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 November 2018, 20:40 UTC
- Waktu yang telah diedit: 23 September 2019 02.37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ecs:DescribeServices",
        "ecs:CreateTaskSet",
        "ecs:UpdateServicePrimaryTaskSet",
        "ecs:DeleteTaskSet",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:ModifyRule",
        "lambda:InvokeFunction",
        "cloudwatch:DescribeAlarms",
        "sns:Publish",
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCodeDeployRoleForECSLimited

`AWSCodeDeployRoleForECSLimited`adalah kebijakanAWS terkelola yang: Menyediakan akses terbatas CodeDeploy layanan untuk melakukan penyebaran biru/hijau ECS atas nama Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeDeployRoleForECSLimited` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 November 2018, 20:42 UTC
- Waktu yang telah diedit: 23 September 2019 07.10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ecs:DescribeServices",
        "ecs:CreateTaskSet",
        "ecs:UpdateServicePrimaryTaskSet",
        "ecs:DeleteTaskSet",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:CodeDeployTopic_*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:ModifyRule"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
```

```
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      },
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsTaskExecutionRole",
        "arn:aws:iam::*:role/ECSTaskExecution*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCodeDeployRoleForLambda

`AWSCodeDeployRoleForLambda`adalah kebijakanAWS terkelola yang: Menyediakan akses CodeDeploy layanan untuk melakukan penerapan Lambda atas nama Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeDeployRoleForLambda` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 28 November 2017, 14:05 UTC
- Waktu yang telah diedit: 03 Desember 2019 19.53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "lambda:UpdateAlias",
        "lambda:GetAlias",
        "lambda:GetProvisionedConcurrencyConfig",
        "sns:Publish"
      ],
      "Resource" : "*",
```

```
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      },
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCodeDeployRoleForLambdaLimited

`AWSCodeDeployRoleForLambdaLimited`adalah kebijakanAWS terkelola yang: Menyediakan akses terbatas CodeDeploy layanan untuk melakukan penerapan Lambda atas nama Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeDeployRoleForLambdaLimited` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 Agustus 2020, 17:14 UTC
- Waktu yang telah diedit: 17 Agustus 2020, 17.14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "lambda:UpdateAlias",
        "lambda:GetAlias",
        "lambda:GetProvisionedConcurrencyConfig"
```

```
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      },
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCodePipeline_FullAccess

`AWSCodePipeline_FullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh AWS CodePipeline melalui AWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSCodePipeline_FullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 03 Agustus 2020, 22:38 UTC
- Waktu telah diedit: 14 Maret 2024, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ListChangeSets",
        "cloudtrail:DescribeTrails",
        "codebuild:BatchGetProjects",
        "codebuild:CreateProject",
        "codebuild:ListCuratedEnvironmentImages",
        "codebuild:ListProjects",
        "codecommit:ListBranches",
```

```
        "codecommit:GetReferences",
        "codecommit:ListRepositories",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:ListClusters",
        "ecs:ListServices",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeEnvironments",
        "iam:ListRoles",
        "iam:GetRole",
        "lambda:ListFunctions",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:DescribeRule",
        "opsworks:DescribeApps",
        "opsworks:DescribeLayers",
        "opsworks:DescribeStacks",
        "s3:ListAllMyBuckets",
        "sns:ListTopics",
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes",
        "states:ListStateMachines"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "CodePipelineAuthoringAccess"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketPolicy",
        "s3:GetBucketVersioning",
        "s3:GetObjectVersion",
        "s3:CreateBucket",
        "s3:PutBucketPolicy"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3::*:codepipeline-*",
      "Sid" : "CodePipelineArtifactsReadWriteAccess"
    },
    {
      "Action" : [
        "cloudtrail:PutEventSelectors",
        "cloudtrail:CreateTrail",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:StartLogging"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudtrail:*:*:trail/codepipeline-source-trail",
      "Sid" : "CodePipelineSourceTrailReadWriteAccess"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/cwe-role-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "events.amazonaws.com"
          ]
        }
      },
      "Sid" : "EventsIAMPassRole"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "codepipeline.amazonaws.com"
          ]
```

```
        }
      },
      "Sid" : "CodePipelineIAMPassRole"
    },
    {
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:DisableRule",
        "events:RemoveTargets"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:events:*:*:rule/codepipeline-*"
      ],
      "Sid" : "CodePipelineEventsReadWriteAccess"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codepipeline:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
```

```
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSCodePipeline_ReadOnlyAccess

`AWSCodePipeline_ReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya bacaAWS CodePipeline melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodePipeline_ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 Agustus 2020, 22:25 UTC
- Waktu yang telah diedit: 03 Agustus 2020, 22.25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListActionExecutions",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "s3:ListAllMyBuckets",
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3::*:codepipeline-*"
    },
    {
      "Sid" : "CodeStarNotificationsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codepipeline:*"
        }
      }
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCodePipelineApproverAccess

`AWSCodePipelineApproverAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk melihat dan menyetujui perubahan manual untuk semua saluran pipa

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodePipelineApproverAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 28 Juli 2016, 18:59 UTC
- Waktu yang telah diedit: 02 Agustus 2017 07.24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCodePipelineCustomActionAccess

`AWSCodePipelineCustomActionAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk tindakan kustom untuk polling untuk rincian pekerjaan (termasuk kredensi sementara) dan melaporkan pembaruan status keAWS CodePipeline.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodePipelineCustomActionAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 Juli 2015, 17:02 UTC
- Waktu yang telah diedit: 09 Juli 2015, 17.02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCodeStarFullAccess

`AWSCodeStarFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS CodeStar melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeStarFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 19 April 2017, 16:23 UTC
- Waktu yang telah diedit: 28 Maret 2023, 00.06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeStarFullAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeStarEC2",
      "Effect" : "Allow",
      "Action" : [
        "codestar:*",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "cloud9:DescribeEnvironment*",
        "cloud9:ValidateEnvironmentName"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarCF",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:ListStacks*",
        "cloudformation:GetTemplateSummary"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCodeStarNotificationsServiceRolePolicy

`AWSCodeStarNotificationsServiceRolePolicy`adalah kebijakanAWS terkelola yang: MemungkinkanAWS CodeStar Pemberitahuan untuk mengakses Amazon CloudWatch Events atas nama Anda

Menggunakan

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan pada pengguna, atau peran Anda.

Perincian detail detail

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 November 2019, 16:10 UTC
- Waktu yang telah diedit: 19 Maret 2020, 16.01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi terkelar ke versi yang menentukan izin untuk Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DescribeRule"
```

```
      ],
      "Resource" : "arn:aws:events:*:*:rule/awscodestarnotifications-*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:CodeStarNotifications-*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommentsForComparedCommit",
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:UpdateSlackChannelConfiguration",
        "codecommit:GetDifferences",
        "codepipeline:ListActionExecutions"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "codecommit:GetFile"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/ExcludeFileContentFromNotifications" : "true"
        }
      },
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCodeStarServiceRole

`AWSCodeStarServiceRole`adalah kebijakanAWS terkelola yang: JANGAN GUNAKAN - Kebijakan PeranAWS CodeStar Layanan yang memberikan hak administratif CodeStar untuk mengelola IAM dan sumber daya layanan lainnya atas nama pelanggan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCodeStarServiceRole` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 April 2017, 15:20 UTC
- Waktu yang telah diedit: 20 September 2021 19.11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole`

Versi kebijakan

Versi kebijakan:v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProjectEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:RemoveTargets",
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule"
      ],
```

```
      "Resource" : [
        "arn:aws:events:*:*:rule/awscodestar-*"
      ]
    },
    {
      "Sid" : "ProjectStack",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*Stack*",
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:GetTemplate"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*",
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/aws-cloud9-*",
        "arn:aws:cloudformation:*:aws:transform/CodeStar*"
      ]
    },
    {
      "Sid" : "ProjectStackTemplate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeChangeSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ProjectQuickstarts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::awscodestar-*/*"
      ]
    },
    {
      "Sid" : "ProjectS3Buckets",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:*"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-codestar-*",
        "arn:aws:s3:::elasticbeanstalk-*"
      ]
    },
    {
      "Sid" : "ProjectServices",
      "Effect" : "Allow",
      "Action" : [
        "codestar:*",
        "codecommit:*",
        "codepipeline:*",
        "codedeploy:*",
        "codebuild:*",
        "autoscaling:*",
        "cloudwatch:Put*",
        "ec2:*",
        "elasticbeanstalk:*",
        "elasticloadbalancing:*",
        "iam:ListRoles",
        "logs:*",
        "sns:*",
        "cloud9:CreateEnvironmentEC2",
        "cloud9:DeleteEnvironment",
        "cloud9:DescribeEnvironment*",
        "cloud9:ListEnvironments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ProjectWorkerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRole",
        "iam:PassRole",
        "iam:GetRolePolicy",
        "iam:PutRolePolicy",
```

```
        "iam:SetDefaultPolicyVersion",
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CodeStarWorker*",
        "arn:aws:iam::*:policy/CodeStarWorker*",
        "arn:aws:iam::*:instance-profile/awscodestar-*"
      ]
    },
    {
      "Sid" : "ProjectTeamMembers",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachUserPolicy",
        "iam:DetachUserPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyArn" : [
            "arn:aws:iam::*:policy/CodeStar_*"
          ]
        }
      }
    },
    {
      "Sid" : "ProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicyVersions",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:policy/CodeStar_*"
      ]
    },
    {
      "Sid" : "InspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-codestar-service-role",
        "arn:aws:iam::*:role/service-role/aws-codestar-service-role"
      ]
    },
    {
      "Sid" : "IAMLinkRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DescribeConfigRuleForARN",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ProjectCodeStarConnections",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codestar-connections:GetConnection"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ProjectCodeStarConnectionsPassConnections",
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCompromisedKeyQuarantine

`AWSCompromisedKeyQuarantine`adalah kebijakanAWS terkelola yang: Menolak akses ke tindakan tertentu, diterapkan olehAWS tim jika kredensi pengguna IAM telah disusupi atau diekspos secara publik. JANGAN hapus kebijakan ini. Sebagai gantinya, ikuti petunjuk yang ditentukan dalam email yang dikirimkan kepada Anda mengenai acara ini.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCompromisedKeyQuarantine` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Agustus 2020, 18:04 UTC
- Waktu yang telah diedit: 11 Agustus 2020, 18.04 UTC

- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateUser",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "lambda:CreateFunction",
        "lightsail:Create*",
        "lightsail:Start*",
```

```
        "lightsail:Delete*",
        "lightsail:Update*",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:DownloadDefaultKeyPair"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSCompromisedKeyQuarantineV2

`AWSCompromisedKeyQuarantineV2`adalah kebijakanAWS terkelola yang: Menolak akses ke tindakan tertentu, diterapkan olehAWS tim jika kredensi pengguna IAM telah disusupi atau diekspos secara publik. JANGAN hapus kebijakan ini. Sebagai gantinya, ikuti petunjuk yang ditentukan dalam kasus dukungan yang dibuat untuk Anda mengenai acara ini.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCompromisedKeyQuarantineV2` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 21 April 2021, 22:30 UTC
- Waktu yang diedit: 16 Maret 2023, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreatePolicyVersion",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PassRole",
        "iam:PutGroupPolicy",
        "iam:PutRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateLoginProfile",
        "iam:UpdateUser",
```

```
        "lambda:AddLayerVersionPermission",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetPolicy",
        "lambda:ListTags",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lightsail:Create*",
        "lightsail:Delete*",
        "lightsail:DownloadDefaultKeyPair",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:Start*",
        "lightsail:Update*",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketAcl",
        "s3:PutBucketOwnershipControls",
        "s3:DeleteBucketPolicy",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:ListAllMyBuckets",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:AcceptReservedInstancesExchangeQuote",
        "ec2:CreateReservedInstancesListing",
        "savingsplans:CreateSavingsPlan"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSConfigMultiAccountSetupPolicy

`AWSConfigMultiAccountSetupPolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Config untuk memanggilAWS layanan dan menyebarkan sumber daya konfigurasi di seluruh organisasi

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 Juni 2019, 18:03 UTC
- Waktu yang telah diedit: 24 Pebruari 2023, 01:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/config-
multiaccountsetup.amazonaws.com/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack",
        "config:DeleteConformancePack"
      ],
      "Resource" : "arn:aws:config:*:*:conformance-pack/aws-service-conformance-pack/
config-multiaccountsetup.amazonaws.com/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "config:DescribeConformancePackStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "config-conforms.amazonaws.com"
        }
      }
    },
    {
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSConfigRemediationServiceRolePolicy

`AWSConfigRemediationServiceRolePolicy`adalah kebijakanAWS terkelola yang: MemungkinkanAWS Config untuk memulihkan sumber daya yang tidak patuh atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran tertaut layanan yang mengizinkan layanan yang mengizinkan layanan yang mengizinkan layanan yang mengizinkan layanan yang mengizinkan layanan yang mengizinkan layanan yang mengizinkan layanan yang mengizinkan Anda tidak dapat melampirkan pada pengguna, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup

Kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 Juni 2019, 21:21 UTC
- Waktu yang telah diedit: 18 Juni 2019, 21.21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Kebijakan ini adalah versi yang menentukan izin. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument",
```

```
        "ssm:StartAutomationExecution"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      },
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSConfigRoleForOrganizations

`AWSConfigRoleForOrganizations`adalah kebijakanAWS terkelola yang: MemungkinkanAWS Config untuk memanggil APIAWS Organizations hanya-baca

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSConfigRoleForOrganizations` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Maret 2018, 22:53 UTC
- Waktu yang telah diedit: 24 November 2020, 20.19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSConfigRulesExecutionRole

`AWSConfigRulesExecutionRole`adalah kebijakanAWS terkelola yang: Memungkinkan fungsiAWS Lambda mengaksesAWS Config API dan snapshot konfigurasi yang diberikanAWS Config secara berkala ke Amazon S3. Akses ini diperlukan oleh fungsi yang mengevaluasi perubahan konfigurasi untuk aturan Config kustom.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSConfigRulesExecutionRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 25 Maret 2016, 17:59 UTC
- Waktu yang telah diedit: 13 Mei 2019 21.33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/AWSLogs/*/Config/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:Put*",
        "config:Get*",
        "config:List*",
        "config:Describe*",
        "config:BatchGet*",
```

```
        "config:Select*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSConfigServiceRolePolicy

`AWSConfigServiceRolePolicy`adalah kebijakan AWS terkelola yang: Mengizinkan Config memanggil AWS layanan dan mengumpulkan konfigurasi sumber daya atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 Mei 2018, 23:31 UTC
- Waktu telah diedit: 22 Februari 2024, 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v50 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigServiceRolePolicyStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListThemes",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListEventIntegrationAssociations",
        "app-integrations:ListEventIntegrations",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
```

```
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "appmesh:DescribeGatewayRoute",
        "appmesh:DescribeMesh",
        "appmesh:DescribeRoute",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApiCache",
```

```
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "APS:DescribeRuleGroupsNamespace",
        "APS:DescribeWorkspace",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListTagsForResource",
        "APS:ListWorkspaces",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:ListAssessments",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
```

```
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cassandra:Select",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListTypes",
        "cloudfront:GetFunction",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:ListDistributions",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetTrailStatus",
```

```
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeRepository",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListReportGroups",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codedeploy:GetDeploymentConfig",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelines",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
```

```
        "cognito-idp:GetGroup",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config:Select*",
        "connect:DescribeEvaluationForm",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribePhoneNumber",
        "connect:DescribePrompt",
        "connect:DescribeQuickConnect",
        "connect:DescribeRule",
        "connect:DescribeUser",
        "connect:GetTaskTemplate",
        "connect:ListApprovedOrigins",
        "connect:ListEvaluationForms",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPrompts",
        "connect:ListQuickConnects",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListUsers",
        "connect:SearchAvailablePhoneNumbers",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
```

```
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListLocations",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "detective:ListGraphs",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "dms:DescribeCertificates",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
```

```
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:DescribeClientVpnAuthorizationRules",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeFleets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
```

```
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:ListAddons",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
```

```
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
```

```
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:ListPolicies",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "forecast:ListTagsForResource",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
```

```
        "frauddetector:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
```

```
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetWorkflow",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:ListComponents",
        "greengrass:ListComponentVersions",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
```

```
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatIntelSets",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
```

```
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADevices",
        "iam:ListMFADeviceTags",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
```

```
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:ListAuthorizers",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
```

```
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetPlaybackKeyPair",
```

```
        "ivs:GetRecordingConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:ListConnectors",
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
```

```
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDistributions",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
```

```
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:GetDataProtectionPolicy",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:ListTagsForResource",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListTagsForResource",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeFlow",
        "mediaconnect:ListFlows",
        "mediaconnect:ListTagsForResource",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
```

```
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListPlaybackConfigurations",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "mobiletargeting:GetApp",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaign",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetEmailChannel",
        "mobiletargeting:GetEmailTemplate",
        "mobiletargeting:GetEventStream",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:GetSegment",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTagsForResource",
        "mobiletargeting:ListTemplates",
        "mq:DescribeBroker",
        "mq:ListBrokers",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
```

```
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "opsworks:DescribeInstances",
        "opsworks:DescribeLayers",
        "opsworks:DescribeTimeBasedAutoScaling",
        "opsworks:DescribeVolumes",
        "opsworks:ListTags",
        "organizations:DescribeAccount",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "profile:GetDomain",
        "profile:GetIntegration",
```

```
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:ListAnalyses",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
```

```
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListServices",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListTagsForResource",
```

```
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "robomaker:DescribeRobotApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListRobotApplications",
        "robomaker:ListSimulationApplications",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:GetChange",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListQueryLoggingConfigs",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetResolverDnssecConfig",
```

```
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver:ListTagsForResource",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketNotification",
```

```
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3express:GetBucketPolicy",
        "s3express:ListAllMyDirectoryBuckets",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProject",
```

```
        "sagemaker:DescribeWorkteam",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelines",
        "sagemaker:ListProjects",
        "sagemaker:ListTags",
        "sagemaker:ListWorkteams",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "sdb:GetAttributes",
        "sdb:ListDomains",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:DescribeHub",
        "serviceCatalog:DescribePortfolioShares",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
```

```
        "ses:DescribeReceiptRuleSet",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetEmailTemplate",
        "ses:GetTemplate",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListEmailTemplates",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListTemplates",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeSubscription",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetDocument",
        "ssm:ListDocuments",
        "ssm:ListTagsForResource",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
```

```
        "states:DescribeStateMachine",
        "states:ListActivities",
        "states:ListStateMachines",
        "states:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "waf-regional:GetLoggingConfiguration",
```

```
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSConfigSLRLogStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "AWSConfigSLRLogEventStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    },
    {
      "Sid" : "AWSConfigSLRApiGatewayStatementID",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/clientcertificates",
```

```
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes/*",
        "arn:aws:apigateway:*::/v2/apis",
        "arn:aws:apigateway:*::/v2/apis/*",
        "arn:aws:apigateway:*::/v2/apis/*/integrations",
        "arn:aws:apigateway:*::/v2/apis/*/integrations/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSConfigUserAccess

`AWSConfigUserAccess`adalah kebijakanAWS terkelola bahwa: memberikan akses untuk menggunakanAWS Config, termasuk mencari tag pada sumber daya, dan membaca semua tag. Ini tidak memberikan izin untuk mengkonfigurasiAWS Config, yang membutuhkan hak administratif.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSConfigUserAccess` ke pengguna, grup, dan peran Anda.

detail

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 18 Februari 2015, 19:38 UTC
- Waktu yang telah diedit: 18 Maret 2019, 20.27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConfigUserAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSConnector

`AWSConnector`adalah kebijakan AWS terkelola yang: Mengaktifkan akses baca/tulis yang luas ke SEMUA objek EC2, akses baca/tulis ke bucket S3 dimulai dengan 'import-to-ec2-', dan kemampuan untuk membuat daftar semua bucket S3, agar Konektor mengimpor VM atas nama Anda. AWS

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSConnector` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 11 Februari 2015, 17:14 UTC
- Waktu telah diedit: 28 September 2015, 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConnector`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : "arn:aws:s3:::import-to-ec2-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelConversionTask",
        "ec2:CancelExportTask",
        "ec2:CreateImage",
        "ec2:CreateInstanceExportTask",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteTags",
        "ec2:DeleteVolume",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
```

```
        "ec2:DescribeTags",
        "ec2:DetachVolume",
        "ec2:ImportInstance",
        "ec2:ImportVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ImportImage",
        "ec2:DescribeImportImageTasks",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:CancelImportTask",
        "ec2:ImportSnapshot",
        "ec2:DescribeImportSnapshotTasks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSControlTowerAccountServiceRolePolicy

`AWSControlTowerAccountServiceRolePolicy`adalah kebijakan AWS terkelola yang: Memungkinkan AWS Control Tower untuk memanggil AWS layanan yang menyediakan konfigurasi akun otomatis dan tata kelola terpusat atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 Juni 2023, 22:04 UTC
- Waktu yang telah diedit: 05 Juni 2023, 22.04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutRuleOnSpecificSourcesAndDetailTypes",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "events:source" : "aws.securityhub"
        },
        "Null" : {
          "events:detail-type" : "false"
        },
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com",
          "events:detail-type" : "Security Hub Findings - Imported"
        }
      }
    },
    {
      "Sid" : "AllowOtherOperationsOnRulesManagedByControlTower",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowDescribeOperationsOnRulesManagedByControlTower",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*"
    },
    {
      "Sid" : "AllowControlTowerToPublishSecurityNotifications",
      "Effect" : "Allow",
      "Action" : "sns:publish",
      "Resource" : "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "AllowActionsForSecurityHubIntegration",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:DescribeStandardsControls",
        "securityhub:GetEnabledStandards"
      ],
      "Resource" : "arn:aws:securityhub:*:*:hub/default"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSControlTowerServiceRolePolicy

`AWSControlTowerServiceRolePolicy`adalah kebijakanAWS terkelola yang: Menyediakan akses keAWS Sumber Daya yang dikelola atau digunakan olehAWS Control Tower

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSControlTowerServiceRolePolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 03 Mei 2019, 18:19 UTC
- Waktu yang telah diedit: 12 April 2023, 19.15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v10 (default)

Versi default kebijakan adalah versi yang menentukan izin kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan kebijakan kebijakan kebijakan


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateStackInstances",
        "cloudformation:UpdateStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteStackInstances",
```

```
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackInstances",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateStackInstances",
        "cloudformation:UpdateStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AWSControlTower*/*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/*",
        "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
        "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateTrail",
        "cloudtrail:DeleteTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudtrail:UpdateTrail",
        "cloudtrail:PutEventSelectors",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
        "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-controltower*/*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSControlTowerExecution",
        "arn:aws:iam::*:role/AWSControlTowerBlueprintAccess"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "ec2:DescribeAvailabilityZones",
        "iam:ListRoles",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "organizations:CreateAccount",
        "organizations:DescribeAccount",
        "organizations:DescribeCreateAccountStatus",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListRoots",
        "organizations:MoveAccount",
        "servicecatalog:AssociatePrincipalWithPortfolio"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
```

```
        "iam:GetUser",
        "iam:ListAttachedRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
        "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
        "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigurationAggregator",
        "config:PutConfigurationAggregator",
        "config:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/aws-control-tower" : "managed-by-control-tower"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "config.amazonaws.com",
            "cloudtrail.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "account:EnableRegion",
        "account:ListRegions",
        "account:GetRegionOptStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSCostAndUsageReportAutomationPolicy

`AWSCostAndUsageReportAutomationPolicy`adalah kebijakanAWS terkelola yang: Memberikan izin untuk mendeskripsikan organisasi akun, membuat bucket S3 untuk program MAP dan menerapkan tag padanya, membuat Laporan Biaya dan Penggunaan, dan menjelaskan definisi Laporan Biaya dan Penggunaan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSCostAndUsageReportAutomationPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 November 2021, 21:27 UTC
- Waktu yang telah diedit: 01 November 2021 09.27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketTagging",
        "s3:PutBucketTagging",
        "s3:GetBucketPolicy",
```

```
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:CreateBucket"
      ],
      "Resource" : "arn:aws:s3:::aws-map-cur-bucket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cur:PutReportDefinition",
        "cur:DeleteReportDefinition",
        "cur:DescribeReportDefinitions"
      ],
      "Resource" : "arn:aws:cur:*:*:definition/map-migrated-report"
    },
    {
      "Effect" : "Allow",
      "Action" : "cur:DescribeReportDefinitions",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSDataExchangeFullAccess

`AWSDataExchangeFullAccess`adalah kebijakanAWS terkelola yang: Memberikan akses penuh keAWS Data Exchange danAWS Marketplace tindakan menggunakanAWS Management Console dan SDK. Ini juga menyediakan akses pilih ke layanan terkait yang diperlukan untuk mengambil keuntungan penuh dariAWS Data Exchange.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDataExchangeFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 13 November 2019, 19:27 UTC
- Waktu yang telah diedit: 02 Desember 2021 16.14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeFullAccess`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:StartChangeSet",
```

```
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:CancelAgreementRequest"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSDataExchangeProviderFullAccess

`AWSDataExchangeProviderFullAccess`adalah kebijakanAWS terkelola yang: Memberikan akses penyediaAWS data ke Data Exchange danAWS Marketplace tindakan menggunakanAWS Management Console dan SDK. Ini juga menyediakan akses pilih ke layanan terkait yang diperlukan untuk mengambil keuntungan penuh dariAWS Data Exchange.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDataExchangeProviderFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 13 November 2019, 19:27 UTC
- Waktu yang telah diedit: 15 Maret 2022, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess`

Versi kebijakan

Versi kebijakan:v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateDataSet",
        "dataexchange:CreateRevision",
        "dataexchange:CreateAsset",
        "dataexchange:Get*",
        "dataexchange:Update*",
        "dataexchange:List*",
        "dataexchange:Delete*",
        "dataexchange:TagResource",
        "dataexchange:UntagResource",
        "dataexchange:PublishDataSet",
        "dataexchange:SendApiAsset",
        "dataexchange:RevokeRevision",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "IMPORT_ASSETS_FROM_S3",
            "IMPORT_ASSET_FROM_SIGNED_URL",
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "IMPORT_ASSET_FROM_API_GATEWAY_API",
            "IMPORT_ASSETS_FROM_REDSHIFT_DATA_SHARES"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSDataExchangeReadOnly

`AWSDataExchangeReadOnly`adalah kebijakanAWS terkelola yang: Memberikan akses hanya-baca keAWS Data Exchange danAWS Marketplace tindakan menggunakanAWS Management Console dan SDK.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDataExchangeReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 13 November 2019, 19:27 UTC
- Waktu yang telah diedit: 10 Mei 2021 09.15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeReadOnly`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:Get*",
        "dataexchange:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSDataExchangeSubscriberFullAccess

`AWSDataExchangeSubscriberFullAccess`adalah kebijakanAWS terkelola yang: Memberikan akses pelangganAWS data ke Data Exchange danAWS Marketplace tindakan menggunakanAWS

Management Console dan SDK. Ini juga menyediakan akses pilih ke layanan terkait yang diperlukan untuk mengambil keuntungan penuh dariAWS Data Exchange.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDataExchangeSubscriberFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 13 November 2019, 19:27 UTC
- Waktu yang telah diedit: 29 November 2021 13.00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:Get*",
        "dataexchange:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
```

```
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "EXPORT_REVISIONS_TO_S3"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateEventAction",
        "dataexchange:UpdateEventAction",
        "dataexchange:DeleteEventAction",
        "dataexchange:SendApiAsset"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:CancelAgreementRequest"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSDataLifecycleManagerServiceRole

`AWSDataLifecycleManagerServiceRole`adalah kebijakanAWS terkelola yang: Menyediakan izin yang sesuai untukAWS Data Lifecycle Manager untuk mengambil tindakan padaAWS sumber daya

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDataLifecycleManagerServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Juli 2018, 19:34 UTC
- Waktu yang telah diedit: 19 September 2022, 17.34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole`

Versi kebijakan

Versi kebijakan:v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:EnableFastSnapshotRestores",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DisableFastSnapshotRestores",
```

```
        "ec2:CopySnapshot",
        "ec2:ModifySnapshotAttribute",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-cwe.*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSDataLifecycleManagerServiceRoleForAMIManagement

`AWSDataLifecycleManagerServiceRoleForAMIManagement`adalah kebijakanAWS terkelola yang: Menyediakan izin yang sesuai untukAWS Data Lifecycle Manager untuk mengambil tindakan padaAWS sumber daya untuk Manajemen AMI

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDataLifecycleManagerServiceRoleForAMIManagement` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 21 Oktober 2020, 19:39 UTC
- Waktu yang telah diedit: 19 Agustus 2021 17.03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*::image/*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ResetImageAttribute",
        "ec2:DeregisterImage",
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImageDeprecation",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSDataLifecycleManagerSSMFullAccess

`AWSDataLifecycleManagerSSMFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan izin Amazon Data Lifecycle Manager untuk melakukan tindakan Systems Manager yang diperlukan untuk menjalankan skrip pra dan pasca di semua instans Amazon EC2.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataLifecycleManagerSSMFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 31 Oktober 2023, 20:29 UTC
- Waktu telah diedit: 16 November 2023, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMReadOnlyAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTaggedSSMDocumentsOnly",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DLMScriptsAccess" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSpecificAWSOwnedSSMDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ssm:*:*:document/AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA"
      ]
    },
    {
      "Sid" : "AllowAllEC2Instances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDataPipeline_FullAccess

`AWSDataPipeline_FullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Data Pipeline, akses daftar untuk peran S3, DynamoDB, Redshift, RDS, SNS, dan IAM, dan akses PassRole untuk Peran default.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDataPipeline_FullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan kebijakan kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 19 Januari 2017, 23:14 UTC
- Waktu yang telah diedit: 17 Agustus 2017 18.48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:List*",
        "dynamodb:DescribeTable",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "sns:ListTopics",
        "sns:Subscribe",
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/DataPipelineDefaultRole"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSDataPipeline_PowerUser

`AWSDataPipeline_PowerUser`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Data Pipeline, akses daftar untuk peran S3, DynamoDB, Redshift, RDS, SNS, dan IAM, dan akses PassRole untuk Peran default.

Menggunakan kebijakan kebijakan ini

Anda dapat melampirkan`AWSDataPipeline_PowerUser` ke pengguna, grup, dan peran Anda.

detail kebijakan kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 19 Januari 2017, 23:16 UTC
- Waktu yang telah diedit: 17 Agustus 2017 18.49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan kebijakan adalah izin kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
```

```
        "s3:List*",
        "dynamodb:DescribeTable",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "sns:ListTopics",
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/DataPipelineDefaultRole"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSDataSyncDiscoveryServiceRolePolicy

`AWSDataSyncDiscoveryServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan DataSync Discovery untuk berintegrasi denganAWS layanan lain atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 Maret 2023, 22:19 UTC
- Waktu yang diedit: 20 Maret 2023, 22.19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync:log-stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSDataSyncFullAccess

`AWSDataSyncFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh AWS DataSync dan akses minimal ke dependensinya

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDataSyncFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 18 Januari 2019, 19:40 UTC
- Waktu yang telah diedit: 16 Februari 2024, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataSyncFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "datasync:*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "iam:GetRole",
        "iam:ListRoles",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "outposts:ListOutposts",
```

```
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListRegionalBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataSyncPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "datasync.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDataSyncReadOnlyAccess

`AWSDataSyncReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-bacaAWS DataSync

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDataSyncReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 18 Januari 2019
- Waktu yang telah diedit: 30 Juni 2020, 17.59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:Describe*",
        "datasync:List*",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "iam:GetRole",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "s3:ListAllMyBuckets",
```

```
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSDeepLensLambdaFunctionAccessPolicy

`AWSDeepLensLambdaFunctionAccessPolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini menetapkan izin yang diperlukan oleh fungsi lambda DeepLens Administratif yang berjalan di DeepLens perangkat

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDeepLensLambdaFunctionAccessPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 November 2017, 15:47 UTC
- Waktu yang telah diedit: 11 Juni 2019, 23.11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepLensS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*/*",
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensGreenGrassCloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/greengrass/*"
    },
    {
      "Sid" : "DeepLensAccess",
      "Effect" : "Allow",
      "Action" : [
        "deeplens:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "DeepLensKinesisVideoAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSDeepLensServiceRolePolicy

`AWSDeepLensServiceRolePolicy`adalah kebijakanAWS terkelola yang: MemberikanAWS DeepLens akses keLayanan AWS, sumber daya, dan peran yang dibutuhkan oleh DeepLens dan dependensinya termasuk IoT, S3, GreenGrass danAWS Lambda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDeepLensServiceRolePolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 29 November 2017, 15:46 UTC
- Waktu yang telah diedit: 25 September 2019 19.25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepLensIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*",
        "arn:aws:iot:*:*:cert/*"
      ]
```

```
    },
    {
      "Sid" : "DeepLensIoTCreateCertificateAndPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensIoTAttachCertificatePolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/deeplens*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "DeepLensIoTDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:GetThingShadow",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "DeepLensAccess",
      "Effect" : "Allow",
      "Action" : [
        "deeplens:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucket",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensCreateS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensIAMPassRoleAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "greengrass.amazonaws.com",
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DeepLensIAMLambdaPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSDeepLens*",
        "arn:aws:iam::*:role/service-role/AWSDeepLens*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DeepLensGreenGrassAccess",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:AssociateRoleToGroup",
        "greengrass:AssociateServiceRoleToAccount",
        "greengrass:CreateResourceDefinition",
        "greengrass:CreateResourceDefinitionVersion",
        "greengrass:CreateCoreDefinition",
        "greengrass:CreateCoreDefinitionVersion",
        "greengrass:CreateDeployment",
        "greengrass:CreateFunctionDefinition",
```

```
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:CreateGroup",
        "greengrass:CreateGroupCertificateAuthority",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateLoggerDefinition",
        "greengrass:CreateLoggerDefinitionVersion",
        "greengrass:CreateSubscriptionDefinition",
        "greengrass:CreateSubscriptionDefinitionVersion",
        "greengrass:DeleteCoreDefinition",
        "greengrass:DeleteFunctionDefinition",
        "greengrass:DeleteGroup",
        "greengrass:DeleteLoggerDefinition",
        "greengrass:DeleteSubscriptionDefinition",
        "greengrass:DisassociateRoleFromGroup",
        "greengrass:DisassociateServiceRoleFromAccount",
        "greengrass:GetAssociatedRole",
        "greengrass:GetConnectivityInfo",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetDeviceDefinition",
        "greengrass:GetDeviceDefinitionVersion",
        "greengrass:GetFunctionDefinition",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupCertificateAuthority",
        "greengrass:GetGroupCertificateConfiguration",
        "greengrass:GetGroupVersion",
        "greengrass:GetLoggerDefinition",
        "greengrass:GetLoggerDefinitionVersion",
        "greengrass:GetResourceDefinition",
        "greengrass:GetServiceRoleForAccount",
        "greengrass:GetSubscriptionDefinition",
        "greengrass:GetSubscriptionDefinitionVersion",
        "greengrass:ListCoreDefinitionVersions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeployments",
        "greengrass:ListDeviceDefinitionVersions",
        "greengrass:ListDeviceDefinitions",
        "greengrass:ListFunctionDefinitionVersions",
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroupCertificateAuthorities",
        "greengrass:ListGroupVersions",
        "greengrass:ListGroups",
```

```
        "greengrass:ListLoggerDefinitionVersions",
        "greengrass:ListLoggerDefinitions",
        "greengrass:ListSubscriptionDefinitionVersions",
        "greengrass:ListSubscriptionDefinitions",
        "greengrass:ResetDeployments",
        "greengrass:UpdateConnectivityInfo",
        "greengrass:UpdateCoreDefinition",
        "greengrass:UpdateDeviceDefinition",
        "greengrass:UpdateFunctionDefinition",
        "greengrass:UpdateGroup",
        "greengrass:UpdateGroupCertificateConfiguration",
        "greengrass:UpdateLoggerDefinition",
        "greengrass:UpdateSubscriptionDefinition",
        "greengrass:UpdateResourceDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensLambdaAdminFunctionAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensLambdaUsersFunctionAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
```

```
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "DeepLensSageMakerWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:StopTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensSageMakerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    },
    {
      "Sid" : "DeepLensKinesisVideoStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:DeleteStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/deeplens*/*"
      ]
    },
    {
      "Sid" : "DeepLensKinesisVideoEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kinesisvideo:GetDataEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSDeepRacerAccountAdminAccess

`AWSDeepRacerAccountAdminAccess`adalah kebijakanAWS terkelola yang: akses DeepRacer admin ke semua tindakan termasuk beralih antara mode multiuser dan pengguna tunggal.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDeepRacerAccountAdminAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 28 Oktober 2021, 01:27 UTC
- Waktu yang telah diedit: 28 Oktober 2021 01.27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSDeepRacerCloudFormationAccessPolicy

`AWSDeepRacerCloudFormationAccessPolicy`kebijakanAWS terkelola yang: Mengizinkan CloudFormation untuk membuat dan mengelolaAWS tumpukan dan sumber daya atas nama Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDeepRacerCloudFormationAccessPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 28 Februari 2019, 21:59 UTC
- Waktu yang telah diedit: 14 Juni 2019, 17.02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
```

```
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DetachInternetGateway",
        "ec2:DisassociateRouteTable",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/AWSDeepRacerLambdaAccessRole",
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:GetFunction",
        "lambda:DeleteFunction",
        "lambda:TagResource",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*DeepRacer*",
        "arn:aws:lambda:*:*:function:*Deepracer*",
        "arn:aws:lambda:*:*:function:*deepracer*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:DeleteBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "robomaker:CreateSimulationApplication",
        "robomaker:CreateSimulationApplicationVersion",
        "robomaker:DeleteSimulationApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListSimulationApplications",
        "robomaker:TagResource",
        "robomaker:UpdateSimulationApplication"
      ],
      "Resource" : [
        "arn:aws:robomaker:*:*:/createSimulationApplication",
        "arn:aws:robomaker:*:*:simulation-application/deepracer*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSDeepRacerDefaultMultiUserAccess

`AWSDeepRacerDefaultMultiUserAccess`adalah kebijakanAWS terkelola yang: Akses pengguna DeepRacer MultiUser default untuk menggunakan deepracer dalam mode multi-pengguna

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDeepRacerDefaultMultiUserAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 28 Oktober 2021, 01:27 UTC
- Waktu yang telah diedit: 28 Oktober 2021 01.27 UTC

- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:Add*",
        "deepracer:Remove*",
        "deepracer:Create*",
        "deepracer:Perform*",
        "deepracer:Clone*",
        "deepracer:Get*",
        "deepracer:List*",
        "deepracer:Edit*",
        "deepracer:Start*",
        "deepracer:Set*",
        "deepracer:Update*",
        "deepracer:Delete*",
        "deepracer:Stop*",
        "deepracer:Import*",
        "deepracer:Tag*",
        "deepracer:Untag*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "false"
        },
```

```
        "Bool" : {
          "deepracer:MultiUser" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:GetAccountConfig",
        "deepracer:GetTrack",
        "deepracer:ListTracks",
        "deepracer:TestRewardFunction"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "deepracer:Admin*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSDeepRacerFullAccess

`AWSDeepRacerFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS DeepRacer. Juga menyediakan akses pilih ke layanan terkait (misalnya, S3).

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDeepRacerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 05 Oktober 2020, 22:03 UTC
- Waktu yang telah diedit: 05 Oktober 2020 22.03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:GetBucketAcl",
```

```
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*",
        "arn:aws:s3:::*DeepRacer*/*",
        "arn:aws:s3:::*Deepracer*/*",
        "arn:aws:s3:::*deepracer*/*",
        "arn:aws:s3:::dr-*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSDeepRacerRoboMakerAccessPolicy

`AWSDeepRacerRoboMakerAccessPolicy`adalah kebijakanAWS terkelola yang: Mengizinkan RoboMaker untuk membuat sumber daya yang diperlukan dan memanggilAWS layanan atas nama Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDeepRacerRoboMakerAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 28 Februari 2019, 21:59 UTC
- Waktu yang telah diedit: 28 Februari 2019 21.59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
```

```
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/robomaker/SimulationJobs",
        "arn:aws:logs:*:*:log-group:/aws/robomaker/SimulationJobs:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/DeepRacer" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
```

```
        "kinesisvideo:TagStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/dr-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSDeepRacerServiceRolePolicy

`AWSDeepRacerServiceRolePolicy`adalah kebijakanAWS terkelola yang: Mengizinkan DeepRacer untuk membuat sumber daya yang diperlukan dan memanggilAWS layanan atas nama Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDeepRacerServiceRolePolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 28 Februari 2019, 21:58 UTC
- Waktu yang telah diedit: 12 Juni 2019 20.55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:*",
        "sagemaker:*",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DetectStackDrift",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:DescribeStackResourceDrifts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      },
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSDeepRacer*",
        "arn:aws:iam::*:role/service-role/AWSDeepRacer*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*DeepRacer*",
        "arn:aws:lambda:*:*:function:*Deepracer*",
        "arn:aws:lambda:*:*:function:*deepracer*",
        "arn:aws:lambda:*:*:function:*dr-*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutBucketPolicy",
        "s3:GetBucketAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/DeepRacer" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DeleteStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:GetHLSStreamingSessionURL",
        "kinesisvideo:GetMedia",
        "kinesisvideo:PutMedia",
        "kinesisvideo:TagStream"
      ],
```

```
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/dr-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSDenyAll

`AWSDenyAll`adalah kebijakan AWS terkelola yang: Tolak semua akses.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSDenyAll` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Mei 2019 22:36 UTC
- Waktu telah diedit: 18 Desember 2023, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDenyAll`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DenyAll",
      "Effect" : "Deny",
      "Action" : [
        "*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSDeviceFarmFullAccess

`AWSDeviceFarmFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke semua operasiAWS Device Farm.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDeviceFarmFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 13 Juli 2015, 16:37 UTC
- Waktu yang telah diedit: 13 Juli 2015 16.37 UTC

- ARN: `arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "devicefarm:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSDeviceFarmServiceRolePolicy

`AWSDeviceFarmServiceRolePolicy`adalah kebijakanAWS terkelola yang: Berikan izin keAWS Device Farm untuk memanggil API Jaringan EC2 atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 September 2022, 21:02 UTC
- Waktu yang telah diedit: 20 September 2022, 21.02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSDeviceFarmTestGridServiceRolePolicy

`AWSDeviceFarmTestGridServiceRolePolicy`adalah kebijakanAWS terkelola yang: Berikan izin keAWS Device Farm untuk memanggil API EC2 atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke peran Anda.

Detail kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 Mei 2021
- Waktu yang telah diedit: 26 Mei 2021 22.01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSDirectConnectFullAccess

`AWSDirectConnectFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS Direct Connect melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDirectConnectFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 30 April 2019 15.29 UTC

- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectFullAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSDirectConnectReadOnlyAccess

`AWSDirectConnectReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja keAWS Direct Connect melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDirectConnectReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 18 Mei 2020, 18.48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSDirectConnectServiceRolePolicy

`AWSDirectConnectServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memberikan izinAWS Direct Connect untuk membuat dan mengelolaAWS sumber daya atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 Januari 2021, 18:35 UTC
- Waktu yang telah diedit: 14 Januari 2021 18.35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSDirectoryServiceFullAccess

`AWSDirectoryServiceFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS Directory Service.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDirectoryServiceFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 24 November 2020, 23.24 UTC

- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DescribeSecurityGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "iam:ListRoles",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:sns:*:*:DirectoryMonitoring*"
    },
    {
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "ds.amazonaws.com"
        }
      }
    },
    {
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSDirectoryServiceReadOnlyAccess

`AWSDirectoryServiceReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca keAWS Directory Service.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDirectoryServiceReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 25 September 2018 21.54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:Check*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ds:Verify*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSDiscoveryContinuousExportFirehosePolicy

`AWSDiscoveryContinuousExportFirehosePolicy`adalah kebijakanAWS terkelola yang: Menyediakan akses tulis keAWS sumber daya yang diperlukan untukAWS Discovery Continuous Export

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSDiscoveryContinuousExportFirehosePolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 Agustus 2018, 18:29 UTC
- Waktu yang telah diedit: 08 Juni 2021 17.32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTableVersions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
```

```
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-application-discovery-service-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/firehose:log-
stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSDMSFleetAdvisorServiceRolePolicy

`AWSDMSFleetAdvisorServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan DMS Fleet Advisor untuk mengelola CloudWatch metrik atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan

- Waktu pembuatan: 06 Maret 2023, 09:10 UTC
- Waktu yang telah diedit: 06 Maret 2023, 09:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan J

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/DMS/FleetAdvisor"
      }
    }
  }
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSDMSServerlessServiceRolePolicy

`AWSDMSServerlessServiceRolePolicy`adalah kebijakan AWS terkelola yang: Memberikan izin AWS DMS Tanpa Server untuk membuat dan mengelola sumber daya DMS di akun Anda atas nama Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, grup, atau peran baru.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 Mei 2023, 20:28 UTC
- Waktu yang telah diedit: 18 Mei 2023, 20.28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi kebijakan ini adalah versi yang mengizinkan untuk kebijakan ini. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "id0",
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationInstance",
        "dms:CreateReplicationTask"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dms:req-tag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id1",
      "Effect" : "Allow",
      "Action" : [
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "id2",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTask",
        "dms:StopReplicationTask",
        "dms:DeleteReplicationTask",
        "dms:DeleteReplicationInstance"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:task:*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id3",
      "Effect" : "Allow",
      "Action" : [
        "dms:TestConnection",
        "dms:DeleteConnection"
      ],
      "Resource" : [
```

```
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:endpoint:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSEC2CapacityReservationFleetRolePolicy

`AWSEC2CapacityReservationFleetRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan layanan CapacityReservation Armada EC2 untuk mengelola Reservasi Kapasitas

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 29 September 2021, 14:43 UTC
- Waktu yang telah diedit: 29 September 2021 14.43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateCapacityReservation",
        "ec2:CancelCapacityReservation",
        "ec2:ModifyCapacityReservation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:CapacityReservationFleet" : "arn:aws:ec2:*:*:capacity-reservation-fleet/
crf-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateCapacityReservation"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSEC2FleetServiceRolePolicy

`AWSEC2FleetServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Armada EC2 untuk meluncurkan dan mengelola instance.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, peran Anda.

Rincian kebijakan JSON

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Maret 2018, 00:08 UTC
- Waktu yang telah diedit: 04 Mei 2020, 20.10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan kebijakan ini adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON SON SON SON SON SON SON SON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2SpotManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
```

```
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2:fleet-id" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSEC2SpotFleetServiceRolePolicy

`AWSEC2SpotFleetServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan EC2 Spot Fleet untuk meluncurkan dan mengelola instance spot fleet

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 Oktober 2017, 19:13 UTC
- Waktu yang telah diedit: 16 Maret 2020, 19.16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan ini adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:spot-instances-request/*",
        "arn:aws:ec2:*:*:spot-fleet-request/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSEC2SpotServiceRolePolicy

`AWSEC2SpotServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan EC2 Spot untuk meluncurkan dan mengelola instans spot

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 September 2017, 18:51 UTC
- Waktu yang telah diedit: 12 Desember 2018, 00:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
```

```
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "ec2:InstanceMarketType" : "spot"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSECRPullThroughCache_ServiceRolePolicy

`AWSECRPullThroughCache_ServiceRolePolicy`adalah kebijakan AWS terkelola yang: Mengaktifkan akses ke AWS layanan dan sumber daya yang digunakan atau dikelola oleh AWS ECR tarik melalui cache

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 November 2021 21:51 UTC
- Waktu yang telah diedit: 13 November 2023, 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "ECR",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecr-pullthroughcache/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticBeanstalkCustomPlatformforEC2Role

`AWSElasticBeanstalkCustomPlatformforEC2Role`adalah kebijakanAWS terkelola yang: Berikan instans dalam izin lingkungan pembuat platform khusus Anda untuk meluncurkan instans EC2, membuat snapshot EBS dan AMI, streaming log ke Amazon CloudWatch Logs, dan menyimpan artefak di Amazon S3.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElasticBeanstalkCustomPlatformforEC2Role` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 21 Februari 2017, 22:50 UTC
- Waktu yang telah diedit: 21 Februari 2017 09.50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Access",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CreateKeypair",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteKeypair",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSnapshot",
```

```
        "ec2:DeleteVolume",
        "ec2:DeregisterImage",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "ec2:GetPasswordData",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySnapshotAttribute",
        "ec2:RegisterImage",
        "ec2:RunInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/platform/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSElasticBeanstalkEnhancedHealth

`AWSElasticBeanstalkEnhancedHealth`adalah kebijakanAWS terkelola yang: Kebijakan PelayananAWS Elastic Beanstalk untuk sistem Pemantauan Health

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElasticBeanstalkEnhancedHealth` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 08 Februari 2016, 23:17 UTC
- Waktu yang telah diedit: 09 April 2018 08.08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:GetConsoleOutput",
        "ec2:AssociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeSecurityGroups",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeNotificationConfigurations",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*:log-stream:*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSElasticBeanstalkMaintenance

`AWSElasticBeanstalkMaintenance`adalah kebijakanAWS terkelola yang: Kebijakan Peran LayananAWS Elastic Beanstalk yang memberikan izin terbatas untuk memperbarui sumber daya Anda atas nama Anda untuk tujuan pemeliharaan.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan JJMMX

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 11 Januari 2019, 23:22 UTC
- Waktu yang telah diedit: 04 Juni 2019 17.48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default JJK adalah versi yang menentukan izin untuk kebijakan default. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationChangeSetOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowElasticBeanstalkStacksUpdateExecuteSuccessfully",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

`AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini untuk peran layananAWS Elastic Beanstalk yang digunakan untuk melakukan pembaruan terkelola lingkungan Elastic Beanstalk. Kebijakan ini tidak boleh dilampirkan

ke pengguna atau peran lain. Kebijakan ini memberikan izin luas untuk membuat dan mengelola sumber daya di sejumlahAWS layanan termasuk AutoScaling, EC2, ECS, Elastic Load Balancing dan CloudFormation. Kebijakan ini juga memungkinkan pengalihan peran IAM apa pun yang dapat digunakan dengan layanan tersebut.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 Maret 2021, 22:18 UTC
- Waktu yang telah diedit: 23 Maret 2023, 23.15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticBeanstalkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScheduledActions",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "logs:DescribeLogGroups",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2BroadOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteSecurityGroup",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2RunInstancesOperationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
```

```
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "EC2TerminateInstancesOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
    {
      "Sid" : "ECSBroadOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:DescribeClusters",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECSDeleteClusterOperationPermissions",
      "Effect" : "Allow",
      "Action" : "ecs:DeleteCluster",
      "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
    },
    {
      "Sid" : "ASGOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
```

```
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:ResumeProcesses",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Sid" : "CFNOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "ELBOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
```

```
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/eb-*/*"
      ]
    },
    {
      "Sid" : "CWLogsOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "S3ObjectOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Sid" : "S3BucketOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
```

```
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "SNSOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Subscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
    },
    {
      "Sid" : "SQSOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:awseb-e-*",
        "arn:aws:sqs:*:*:eb-*"
      ]
    },
    {
      "Sid" : "CWPutMetricAlarmOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:awseb-*",
        "arn:aws:cloudwatch:*:*:alarm:eb-*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

`AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`adalah kebijakanAWS terkelola yang: kebijakan Peran LayananAWS Elastic Beanstalk yang memberikan izin terbatas untuk pembaruan terkelola.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau pengguna, atau pengguna, atau kebijakan ini ke pengguna, atau atau pengguna, atau atau kebijakan ini.

detail kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 November 2019, 22:35 UTC
- Waktu yang diedit: 24 Maret 2023, 00:18 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SingleInstanceAPIs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:releaseAddress",
        "ec2:allocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterTaskDefinition",
        "ecs:DeRegisterTaskDefinition",
        "ecs:List*",
        "ecs:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElasticBeanstalkAPIs",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyAPIs",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:List*",
        "ec2:Describe*",
        "autoscaling:Describe*",
        "elasticloadbalancing:Describe*",
        "logs:DescribeLogGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
```

```
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Sid" : "CFN",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CancelUpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-e-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
    {
      "Sid" : "S3Obj",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Sid" : "S3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "CWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "ELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeRegisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-e-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*"
      ]
    },
    {
      "Sid" : "SNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-Environment-*"
    },
    {
      "Sid" : "EC2LaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*"
    },
    {
      "Sid" : "AllowLaunchTemplateRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
```

```
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RegisterTaskDefinition"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSElasticBeanstalkMulticontainerDocker

`AWSElasticBeanstalkMulticontainerDocker`adalah kebijakanAWS terkelola yang: Menyediakan instans dalam akses lingkungan Docker multicontainer Anda untuk menggunakan Amazon EC2 Container Service untuk mengelola tugas penyebaran kontainer.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElasticBeanstalkMulticontainerDocker` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 Februari 2016, 23:15 UTC
- Waktu yang telah diedit: 23 Maret 2023, 22.04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecs:Poll",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:DiscoverPollEndpoint",
        "ecs:StartTelemetrySession",
        "ecs:RegisterContainerInstance",
        "ecs:DeregisterContainerInstance",
        "ecs:DescribeContainerInstances",
        "ecs:Submit*",
        "ecs:DescribeTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RegisterContainerInstance",
            "StartTask"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSElasticBeanstalkReadOnly

`AWSElasticBeanstalkReadOnly`adalah kebijakanAWS terkelola yang: Memberikan izin hanya-baca. Secara eksplisit memungkinkan operator untuk mendapatkan akses langsung untuk mengambil informasi tentang sumber daya yang terkait dengan aplikasiAWS Elastic Beanstalk.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElasticBeanstalkReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 22 Januari 2021, 19:02 UTC
- Waktu yang telah diedit: 22 Januari 2021 07.02 UTC

- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAPIs",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScheduledActions",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ValidateTemplate",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
```

```
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribeDBSnapshots",
        "s3:ListAllMyBuckets",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSElasticBeanstalkRoleCore

`AWSElasticBeanstalkRoleCore`adalah kebijakanAWS terkelola yang: AWSElasticBeanstalkRoleCore (Elastic Beanstalk operations role) Memungkinkan operasi inti dari lingkungan layanan web.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElasticBeanstalkRoleCore` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2020, 21:48 UTC
- Waktu yang telah diedit: 09 September 2020 20.31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/awseb-e-*"
        }
      }
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReleaseAddress",
        "ec2:AllocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroup*",
        "ec2:RevokeSecurityGroup*",
        "ec2:CreateLaunchTemplate*",
        "ec2:DeleteLaunchTemplate*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LTRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:*LoadBalancer*",
        "autoscaling:*AutoScalingGroup",
        "autoscaling:*LaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:*Tags"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*"
      ]
    },
    {
      "Sid" : "ASGPolicy",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeletePolicy"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "EBSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticbeanstalk.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Obj",
      "Effect" : "Allow",
      "Action" : [
        "s3:Delete*",
        "s3:Get*",
        "s3:Put*"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*/*",
        "arn:aws:s3:::elasticbeanstalk-env-resources-*/*"
      ]
    },
    {
      "Sid" : "S3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucket*",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "CFN",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:UpdateStack",
        "cloudformation:ContinueUpdateRollback",
        "cloudformation:CancelUpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/awseb-e-*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:awseb-*"
    },
    {
      "Sid" : "ELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Create*",
        "elasticloadbalancing:Delete*",
        "elasticloadbalancing:Modify*",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeRegisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:*Tags",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:SetRulePriorities",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/awseb-*",
```

```
        "arn:aws:elasticloadbalancing:*:*:listener/net/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/*/*/*"
      ]
    },
    {
      "Sid" : "ListAPIs",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "logs:Describe*",
        "ec2:Describe*",
        "ecs:Describe*",
        "ecs:List*",
        "elasticloadbalancing:Describe*",
        "rds:Describe*",
        "sns:List*",
        "iam:List*",
        "acm:Describe*",
        "acm:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSElasticBeanstalkRoleCWL

`AWSElasticBeanstalkRoleCWL`adalah kebijakanAWS terkelola yang: (Peran operasi Elastic Beanstalk) Memungkinkan lingkungan untuk mengelola grup CloudWatch log Amazon Logs.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElasticBeanstalkRoleCWL` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2020, 21:49 UTC
- Waktu yang telah diedit: 05 Juni 2020, 21.49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSElasticBeanstalkRoleECS

`AWSElasticBeanstalkRoleECS`adalah kebijakanAWS terkelola yang: (Peran operasi Elastic Beanstalk) Memungkinkan lingkungan Docker multicontainer untuk mengelola klaster Amazon ECS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElasticBeanstalkRoleECS` ke pengguna, grup, dan peran Anda.

detail

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2020, 21:47 UTC
- Waktu yang telah diedit: 23 Maret 2023, 22.43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
        "ecs:RegisterTaskDefinition",
        "ecs:DeRegisterTaskDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSElasticBeanstalkRoleRDS

`AWSElasticBeanstalkRoleRDS`adalah kebijakanAWS terkelola yang: (Peran operasi Elastic Beanstalk) Memungkinkan lingkungan untuk mengintegrasikan instans Amazon RDS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElasticBeanstalkRoleRDS` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2020, 21:46 UTC
- Waktu yang telah diedit: 05 Juni 2020, 21.46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "AllowRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBSecurityGroup",
        "rds:DeleteDBSecurityGroup",
        "rds:AuthorizeDBSecurityGroupIngress",
        "rds:CreateDBInstance",
        "rds:ModifyDBInstance",
        "rds:DeleteDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:secgrp:awseb-e-*",
        "arn:aws:rds:*:*:db:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSElasticBeanstalkRoleSNS

`AWSElasticBeanstalkRoleSNS`Adalah kebijakanAWS terkelola yang: (Peran operasi Elastic Beanstalk) Memungkinkan lingkungan untuk mengaktifkan integrasi topik Amazon SNS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElasticBeanstalkRoleSNS` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2020, 21:46 UTC

- Waktu yang telah diedit: 05 Juni 2020, 21.46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowBeanstalkManageSNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes",
        "sns:DeleteTopic"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
      ]
    },
    {
      "Sid" : "AllowSNSPublish",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSElasticBeanstalkRoleWorkerTier

`AWSElasticBeanstalkRoleWorkerTier`adalah kebijakanAWS terkelola yang: (Peran operasi Elastic Beanstalk) Memungkinkan tingkat lingkungan pekerja untuk membuat tabel Amazon DynamoDB dan antrean Amazon SQS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElasticBeanstalkRoleWorkerTier` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2020, 21:43 UTC
- Waktu yang telah diedit: 05 Juni 2020, 21.43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSQS",
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:CreateQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:awseb-e-*"
    },
    {
      "Sid" : "AllowDDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:TagResource",
        "dynamodb:DescribeTable",
        "dynamodb:DeleteTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/awseb-e-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSElasticBeanstalkService

`AWSElasticBeanstalkService`adalah kebijakanAWS terkelola yang: Kebijakan ini berada di jalur pengusangan. Lihat dokumentasi untuk panduan: https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html. AWS Kebijakan peran Layanan Elastic Beanstalk yang memberikan

izin untuk membuat & mengelola sumber daya (yaitu:AutoScaling, EC2, S3,CloudFormation, ELB, dll.) Atas nama Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElasticBeanstalkService` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 April 2016, 20:27 UTC
- Waktu yang telah diedit: 10 Mei 2023, 19.29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

Versi kebijakan

Versi kebijakan:v17 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowDeleteCloudwatchLogGroups",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    },
    {
      "Sid" : "AllowS3OperationsOnElasticBeanstalkBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:*"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "AllowLaunchTemplateRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
```

```
      }
    },
    {
      "Sid" : "AllowELBAddTags",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOperations",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DetachInstances",
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:ResumeProcesses",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:SuspendProcesses",
```

```
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup",
        "cloudwatch:PutMetricAlarm",
        "ec2:AssociateAddress",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeVpcClassicLink",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:TerminateInstances",
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
        "ecs:DescribeClusters",
        "ecs:RegisterTaskDefinition",
        "elasticbeanstalk:*",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
```

```
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "iam:ListRoles",
        "iam:PassRole",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogGroups",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:ListBucket",
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sns:Subscribe",
        "sns:SetTopicAttributes",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSElasticBeanstalkServiceRolePolicy

`AWSElasticBeanstalkServiceRolePolicy`adalah kebijakanAWS terkelola yang: kebijakanAWS Elastic Beanstalk Service Linked Role yang memberikan izin untuk membuat & mengelola sumber daya (yaitu: AutoScaling, EC2, S3 CloudFormation,, ELB, dll.) atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 September 2017, 23:46 UTC
- Waktu yang telah diedit: 06 Juni 2019, 21.59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationReadOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
```

```
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowOperations",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:PutNotificationConfiguration",
        "ec2:DescribeInstanceStatus",
        "ec2:AssociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "lambda:GetFunction",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowOperationsOnHealthStreamingLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DeleteLogGroup",
        "logs:PutLogEvents"
      ],
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSElasticBeanstalkWebTier

`AWSElasticBeanstalkWebTier`adalah kebijakanAWS terkelola yang: Menyediakan instans dalam akses lingkungan server web Anda untuk mengunggah file log ke Amazon S3.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElasticBeanstalkWebTier` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 Februari 2016, 23:08 UTC
- Waktu yang telah diedit: 09 September 2020 19.38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier`

Versi kebijakan

Versi kebijakan:v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "XRayAccess",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    },
    {
      "Sid" : "ElasticBeanstalkHealthAccess",
      "Action" : [
        "elasticbeanstalk:PutInstanceStatistics"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:elasticbeanstalk:*:*:application/*",
        "arn:aws:elasticbeanstalk:*:*:environment/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSElasticBeanstalkWorkerTier

`AWSElasticBeanstalkWorkerTier`adalah kebijakanAWS terkelola yang: Menyediakan instans di lingkungan pekerja Anda akses untuk mengunggah file log ke Amazon S3, untuk menggunakan Amazon SQS untuk memantau antrean pekerjaan aplikasi Anda, menggunakan Amazon DynamoDB untuk melakukan pemilihan pemimpin, dan CloudWatch ke Amazon untuk mempublikasikan metrik pemantauan kesehatan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElasticBeanstalkWorkerTier` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 Februari 2016, 23:12 UTC
- Waktu yang telah diedit: 09 September 2020 19.53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MetricsAccess",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "XRayAccess",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "QueueAccess",
      "Action" : [
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "DynamoPeriodicTasks",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:DeleteItem",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:UpdateItem"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/*-stack-AWSEBWorkerCronLeaderRegistry*"
      ]
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    },
    {
      "Sid" : "ElasticBeanstalkHealthAccess",
```

```
      "Action" : [
        "elasticbeanstalk:PutInstanceStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:elasticbeanstalk:*:*:application/*",
        "arn:aws:elasticbeanstalk:*:*:environment/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSElasticDisasterRecoveryAgentInstallationPolicy

`AWSElasticDisasterRecoveryAgentInstallationPolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini memungkinkan penginstalan Agen AWS Replikasi, yang digunakan dengan AWS Elastic Disaster Recovery (DRS) untuk memulihkan server eksternal. AWS Lampirkan kebijakan ini ke pengguna IAM Anda atau peran yang kredensialnya Anda berikan selama langkah instalasi Agen Replikasi. AWS

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryAgentInstallationPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2021 10:37 UTC
- Waktu telah diedit: November 27, 2023, 12:38 UTC

- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSAgentInstallationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:CreateSourceServerForDrs",
        "drs:CreateRecoveryInstanceForDrs",
        "drs:DescribeRecoveryInstances",
        "drs:CreateSourceNetwork"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSAgentInstallationPolicy2",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
```

```
      "Sid" : "DRSAgentInstallationPolicy3",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateRecoveryInstanceForDrs"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy4",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-network/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceNetwork"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy5",
      "Effect" : "Allow",
      "Action" : "drs:IssueAgentCertificateForDrs",
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryAgentPolicy

`AWSElasticDisasterRecoveryAgentPolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini memungkinkan penggunaan Agen AWS Replikasi, yang digunakan dengan AWS Elastic Disaster Recovery (DRS) untuk memulihkan server sumber. AWS Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryAgentPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 November 2021 10:32 UTC
- Waktu telah diedit: 27 November 2023, 13:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSAgentPolicy1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs",
        "drs:IssueAgentCertificateForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/${aws:SourceIdentity}"
    },
    {
      "Sid" : "DRSAgentPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryConsoleFullAccess

`AWSElasticDisasterRecoveryConsoleFullAccess`adalah kebijakan AWS terkelola yang: Kebijakan ini menyediakan akses penuh ke semua API publik AWS Elastic Disaster Recovery (DRS), serta izin untuk membaca kunci KMS, License Manager, Resource Groups, Elastic Load Balancing, IAM, dan informasi EC2. Lampirkan kebijakan ini ke pengguna atau peran IAM Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2021 10:46 UTC
- Waktu telah diedit: 16 Oktober 2023, 12:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeHosts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess4",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess5",
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess6",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess7",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess8",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "ConsoleFullAccess10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "ConsoleFullAccess13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess15",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess16",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "ConsoleFullAccess17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
```

```
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
```

```
        "ec2:AttachVolume",
        "ec2:StartInstances",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "ConsoleFullAccess24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess25",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
```

```
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess28",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess29",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryConsoleFullAccess_v2

`AWSElasticDisasterRecoveryConsoleFullAccess_v2`adalah kebijakan AWS terkelola yang: Kebijakan ini menyediakan akses penuh ke semua API publik AWS Elastic Disaster Recovery (AWSDRS), serta semua API publik di AWS layanan lain yang digunakan oleh AWS DRS Console. Lampirkan kebijakan ini ke pengguna atau peran Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryConsoleFullAccess_v2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 November 2023, 13:35 UTC
- Waktu telah diedit: 27 November 2023, 13:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
```

```
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeHosts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess4",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess5",
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess6",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess7",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess8",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
```

```
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "ConsoleFullAccess16",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "ConsoleFullAccess17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
```

```
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:StartInstances",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
```

```
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess25",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances"
          ]
        },
```

```
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess28",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess29",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess30",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
```

```
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess31",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-CreateImage:$DEFAULT",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess32",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess33",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess34",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess35",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
```

```
    {
      "Sid" : "ConsoleFullAccess36",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess37",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryConversionServerPolicy

`AWSElasticDisasterRecoveryConversionServerPolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini dilampirkan ke peran instance server AWS Elastic Disaster Recovery Conversion. Kebijakan ini memungkinkan Server Konversi Elastic Disaster Recovery (DRS), yang merupakan instans EC2 yang diluncurkan oleh Elastic Disaster Recovery, untuk berkomunikasi dengan layanan DRS. Peran IAM dengan kebijakan ini dilampirkan (sebagai Profil Instans EC2) oleh DRS ke Server Konversi DRS, yang secara otomatis diluncurkan dan dihentikan oleh DRS, bila diperlukan. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda. DRS Conversion Server digunakan oleh Elastic Disaster Recovery ketika pengguna memilih untuk memulihkan server sumber menggunakan konsol DRS, CLI, atau API.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryConversionServerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 November 2021 13:42 UTC
- Waktu telah diedit: 27 November 2023, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "DRSConversionServerPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSConversionServerPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

`AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini memungkinkan AWS Elastic Disaster Recovery (DRS) untuk mendukung replikasi lintas akun dan kegagalan lintas akun.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryCrossAccountReplicationPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Mei 2023, 07:16 UTC
- Waktu telah diedit: 17 Januari 2024, 13:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CrossAccountPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeInstances",
        "drs:DescribeSourceServers",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:CreateSourceServerForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccountPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
```

```
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryEc2InstancePolicy

`AWSElasticDisasterRecoveryEc2InstancePolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini memungkinkan penginstalan dan penggunaan Agen AWS Replikasi, yang digunakan oleh AWS Elastic Disaster Recovery (DRS) untuk memulihkan server sumber yang berjalan di EC2 (lintas wilayah atau lintas AZ). Peran IAM dengan kebijakan ini harus dilampirkan (sebagai Profil Instans EC2) ke Instans EC2.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryEc2InstancePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Mei 2022, 12:30 UTC
- Waktu telah diedit: 27 November 2023, 13:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSEc2InstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:CreateSourceServerForDrs",
        "drs:CreateSourceNetwork"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSEc2InstancePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
      "Sid" : "DRSEc2InstancePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
```

```
      ],
      "Resource" : "arn:aws:drs:*:*:source-network/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceNetwork"
        }
      }
    },
    {
      "Sid" : "DRSEc2InstancePolicy4",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSEc2InstancePolicy5",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/DRSCrossAccountAgentAuthorizedRole_*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SourceInstanceARN" : "${ec2:SourceInstanceARN}"
        },
        "ForAnyValue:StringEquals" : {
          "sts:TransitiveTagKeys" : "SourceInstanceARN"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryFailbackInstallationPolicy

`AWSElasticDisasterRecoveryFailbackInstallationPolicy`adalah kebijakan AWS terkelola yang: Anda dapat melampirkan AWSElasticDisasterRecoveryFailbackInstallationPolicy kebijakan ke identitas IAM Anda. Kebijakan ini memungkinkan penginstalan Elastic Disaster Recovery Failback Client, yang digunakan untuk mengembalikan Instans Pemulihan kembali ke infrastruktur sumber asli Anda. Lampirkan kebijakan ini ke pengguna IAM atau peran yang kredensialnya Anda berikan saat menjalankan Klien Kegagalan Pemulihan Bencana Elastis.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryFailbackInstallationPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2021, 11:02 UTC
- Waktu telah diedit: 27 November 2023, 13:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSFailbackInstallationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeSourceServers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackInstallationPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource",
        "drs:IssueAgentCertificateForDrs",
        "drs:AssociateFailbackClientToRecoveryInstanceForDrs",
        "drs:GetSuggestedFailbackClientDeviceMappingForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateFailbackClientDeviceMappingForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryFailbackPolicy

`AWSElasticDisasterRecoveryFailbackPolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini memungkinkan penggunaan Klien Kegagalan Pemulihan Bencana Elastis, yang digunakan untuk mengembalikan Instans Pemulihan kembali ke infrastruktur sumber asli Anda. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryFailbackPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 November 2021 10:41 UTC
- Waktu telah diedit: 27 November 2023, 12:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSFailbackPolicy1",
      "Effect" : "Allow",
```

```
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeReplicationServerAssociationsForDrs",
        "drs:DescribeRecoveryInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetFailbackCommandForDrs",
        "drs:UpdateFailbackClientLastSeenForDrs",
        "drs:NotifyAgentAuthenticationForDrs",
        "drs:UpdateAgentReplicationProcessStateForDrs",
        "drs:NotifyAgentReplicationProgressForDrs",
        "drs:NotifyAgentConnectedForDrs",
        "drs:NotifyAgentDisconnectedForDrs",
        "drs:NotifyConsistencyAttainedForDrs",
        "drs:GetFailbackLaunchRequestedForDrs",
        "drs:IssueAgentCertificateForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/${aws:SourceIdentity}"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryLaunchActionsPolicy

`AWSElasticDisasterRecoveryLaunchActionsPolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini memungkinkan Anda menggunakan Amazon SSM dan layanan tambahan izin yang diperlukan untuk menjalankan tindakan pasca-peluncuran di AWS Elastic Disaster Recovery (AWSDRS). Lampirkan kebijakan ini ke peran atau pengguna IAM Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryLaunchActionsPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 September 2023, 07:38 UTC
- Waktu telah diedit: 16 Oktober 2023, 12:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LaunchActionsPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "LaunchActionsPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-*",
        "arn:aws:ssm:*::document/AWSCodeDeployAgent-*",
        "arn:aws:ssm:*::document/AWSConfigRemediation-*",
        "arn:aws:ssm:*::document/AWSConformancePacks-*",
        "arn:aws:ssm:*::document/AWSDisasterRecovery-*",
        "arn:aws:ssm:*::document/AWSDistroOTel-*",
        "arn:aws:ssm:*::document/AWSDocs-*",
        "arn:aws:ssm:*::document/AWSEC2-*",
        "arn:aws:ssm:*::document/AWSEC2Launch-*",
        "arn:aws:ssm:*::document/AWSFIS-*",
        "arn:aws:ssm:*::document/AWSFleetManager-*",
        "arn:aws:ssm:*::document/AWSIncidents-*",
        "arn:aws:ssm:*::document/AWSKinesisTap-*",
        "arn:aws:ssm:*::document/AWSMigration-*",
        "arn:aws:ssm:*::document/AWSNVMe-*",
        "arn:aws:ssm:*::document/AWSNitroEnclavesWindows-*",
        "arn:aws:ssm:*::document/AWSObservabilityExporter-*",
        "arn:aws:ssm:*::document/AWSPVDriver-*",
        "arn:aws:ssm:*::document/AWSQuickSetupType-*",
        "arn:aws:ssm:*::document/AWSQuickStarts-*",
        "arn:aws:ssm:*::document/AWSRefactorSpaces-*",
        "arn:aws:ssm:*::document/AWSResilienceHub-*",
        "arn:aws:ssm:*::document/AWSSAP-*",
        "arn:aws:ssm:*::document/AWSSAPTools-*",
        "arn:aws:ssm:*::document/AWSSQLServer-*",
        "arn:aws:ssm:*::document/AWSSSO-*",
        "arn:aws:ssm:*::document/AWSSupport-*",
        "arn:aws:ssm:*::document/AWSSystemsManagerSAP-*",
        "arn:aws:ssm:*::document/AmazonCloudWatch-*",
        "arn:aws:ssm:*::document/AmazonCloudWatchAgent-*",
        "arn:aws:ssm:*::document/AmazonECS-*",
        "arn:aws:ssm:*::document/AmazonEFSUtils-*",
        "arn:aws:ssm:*::document/AmazonEKS-*",
        "arn:aws:ssm:*::document/AmazonInspector-*",
        "arn:aws:ssm:*::document/AmazonInspector2-*",
```

```
        "arn:aws:ssm:*::document/AmazonInternal-*",
        "arn:aws:ssm:*::document/AwsEnaNetworkDriver-*",
        "arn:aws:ssm:*::document/AwsVssComponents-*",
        "arn:aws:ssm:*::automation-definition/AWS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSCodeDeployAgent-*:*",
        "arn:aws:ssm:*::automation-definition/AWSConfigRemediation-*:*",
        "arn:aws:ssm:*::automation-definition/AWSConformancePacks-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDisasterRecovery-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDistroOTel-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDocs-*:*",
        "arn:aws:ssm:*::automation-definition/AWSEC2-*:*",
        "arn:aws:ssm:*::automation-definition/AWSEC2Launch-*:*",
        "arn:aws:ssm:*::automation-definition/AWSFIS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSFleetManager-*:*",
        "arn:aws:ssm:*::automation-definition/AWSIncidents-*:*",
        "arn:aws:ssm:*::automation-definition/AWSKinesisTap-*:*",
        "arn:aws:ssm:*::automation-definition/AWSMigration-*:*",
        "arn:aws:ssm:*::automation-definition/AWSNVMe-*:*",
        "arn:aws:ssm:*::automation-definition/AWSNitroEnclavesWindows-*:*",
        "arn:aws:ssm:*::automation-definition/AWSObservabilityExporter-*:*",
        "arn:aws:ssm:*::automation-definition/AWSPVDriver-*:*",
        "arn:aws:ssm:*::automation-definition/AWSQuickSetupType-*:*",
        "arn:aws:ssm:*::automation-definition/AWSQuickStarts-*:*",
        "arn:aws:ssm:*::automation-definition/AWSRefactorSpaces-*:*",
        "arn:aws:ssm:*::automation-definition/AWSResilienceHub-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSAP-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSAPTools-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSQLServer-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSSO-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSupport-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSystemsManagerSAP-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonCloudWatch-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonCloudWatchAgent-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonECS-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonEFSUtils-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonEKS-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInspector-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInspector2-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInternal-*:*",
        "arn:aws:ssm:*::automation-definition/AwsEnaNetworkDriver-*:*",
        "arn:aws:ssm:*::automation-definition/AwsVssComponents-*:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "LaunchActionsPolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LaunchActionsPolicy7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocumentVersions",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "LaunchActionsPolicy8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy9",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy10",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy11",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "drs.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryNetworkReplicationPolicy

`AWSElasticDisasterRecoveryNetworkReplicationPolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini memungkinkan AWS Elastic Disaster Recovery (DRS) untuk mendukung replikasi jaringan.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryNetworkReplicationPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 Juni 2023, 12:36 UTC
- Waktu telah diedit: 02 Januari 2024, 13:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSNetworkReplicationPolicy1",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeInstances",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedPrefixListAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryReadOnlyAccess

`AWSElasticDisasterRecoveryReadOnlyAccess`adalah kebijakan AWS terkelola yang: Anda dapat melampirkan AWSElasticDisasterRecoveryReadOnlyAccess kebijakan ke identitas IAM Anda. Kebijakan ini memberikan izin untuk semua API publik hanya-baca Elastic Disaster Recovery (DRS), serta beberapa API hanya-baca dari AWS layanan lain yang diperlukan untuk menggunakan konsol DRS hanya baca sepenuhnya. Lampirkan kebijakan ini ke pengguna atau peran IAM Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 November 2021 10:50 UTC
- Waktu telah diedit: 27 November 2023, 13:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReadOnlyAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "drs:ListLaunchActions"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "DRSReadOnlyAccess2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess4",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess5",
      "Effect" : "Allow",
      "Action" : "ssm:ListCommandInvocations",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess6",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameter",
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
    },
    {
      "Sid" : "DRSReadOnlyAccess7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-CreateImage",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
```

```
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure"
      ]
    },
    {
      "Sid" : "DRSReadOnlyAccess8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryRecoveryInstancePolicy

`AWSElasticDisasterRecoveryRecoveryInstancePolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini dilampirkan pada peran instans pemulihan Elastic Disaster Recovery. Kebijakan ini memungkinkan Instans Pemulihan Bencana Elastis (DRS), yang merupakan instans EC2 yang diluncurkan oleh Elastic Disaster Recovery - untuk berkomunikasi dengan layanan DRS, dan untuk dapat gagal kembali ke infrastruktur sumber aslinya. Peran IAM dengan kebijakan ini dilampirkan (sebagai Profil Instans EC2) oleh Elastic Disaster Recovery ke Instans Pemulihan DRS. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryRecoveryInstancePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 November 2021 10:20 UTC
- Waktu telah diedit: 27 November 2023, 13:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSRecoveryInstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs",
```

```
        "drs:UpdateReplicationCertificateForDrs",
        "drs:NotifyReplicationServerAuthenticationForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*",
      "Condition" : {
        "StringEquals" : {
          "drs:EC2InstanceARN" : "${ec2:SourceInstanceARN}"
        }
      }
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeRecoveryInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy4",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:CreateSourceServerForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy5",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy6",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy7",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/DRSCrossAccountAgentAuthorizedRole_*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SourceInstanceARN" : "${ec2:SourceInstanceARN}"
        },
        "ForAnyValue:StringEquals" : {
          "sts:TransitiveTagKeys" : "SourceInstanceARN"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryReplicationServerPolicy

`AWSElasticDisasterRecoveryReplicationServerPolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini dilampirkan ke peran instance server Elastic Disaster Recovery Replication. Kebijakan ini memungkinkan Server Replikasi Elastic Disaster Recovery (DRS), yang merupakan instans EC2 yang diluncurkan oleh Elastic Disaster Recovery - untuk berkomunikasi dengan layanan DRS, dan membuat snapshot EBS di situs Anda. Akun AWS Peran IAM dengan kebijakan ini dilampirkan (sebagai Profil Instans EC2) oleh Elastic Disaster Recovery ke Server Replikasi DRS yang secara otomatis diluncurkan dan dihentikan oleh DRS, sesuai kebutuhan. Server Replikasi DRS digunakan untuk memfasilitasi replikasi data dari server eksternal Anda keAWS, sebagai bagian dari proses pemulihan yang dikelola oleh DRS. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryReplicationServerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 November 2021 13:34 UTC
- Waktu telah diedit: 27 November 2023, 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReplicationServerPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentSnapshotCreditsForDrs",
        "drs:DescribeReplicationServerAssociationsForDrs",
        "drs:DescribeSnapshotRequestsForDrs",
        "drs:BatchDeleteSnapshotRequestForDrs",
        "drs:NotifyAgentAuthenticationForDrs",
        "drs:BatchCreateVolumeSnapshotGroupForDrs",
        "drs:UpdateAgentReplicationProcessStateForDrs",
        "drs:NotifyAgentReplicationProgressForDrs",
        "drs:NotifyAgentConnectedForDrs",
        "drs:NotifyAgentDisconnectedForDrs",
        "drs:NotifyVolumeEventForDrs",
        "drs:SendVolumeStatsForDrs"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy5",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSReplicationServerPolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSReplicationServerPolicy7",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryServiceRolePolicy

`AWSElasticDisasterRecoveryServiceRolePolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini memungkinkan Elastic Disaster Recovery untuk mengelola AWS sumber daya atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 November 2021 10:56 UTC
- Waktu telah diedit: 17 Januari 2024, 13:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSServiceRolePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:CreateRecoveryInstanceForDrs",
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy4",
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DRSServiceRolePolicy5",
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeAttribute",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedPrefixListAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "DRSServiceRolePolicy11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy16",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Sid" : "DRSServiceRolePolicy25",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryReplicationServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
```

```
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy28",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryStagingAccountPolicy

`AWSElasticDisasterRecoveryStagingAccountPolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini memungkinkan akses hanya-baca ke sumber daya AWS Elastic Disaster Recovery (DRS) seperti server sumber dan pekerjaan. Ini juga memungkinkan membuat snapshot yang dikonversi dan berbagi snapshot EBS itu dengan akun tertentu.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryStagingAccountPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Mei 2022, 09:49 UTC
- Waktu telah diedit: 27 November 2023, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSStagingAccountPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
        "drs:DescribeJobLogItems"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DRSStagingAccountPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/userId" : "${aws:SourceIdentity}"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

`AWSElasticDisasterRecoveryStagingAccountPolicy_v2`adalah kebijakan AWS terkelola yang: Kebijakan ini digunakan oleh AWS Elastic Disaster Recovery (DRS) untuk memulihkan server sumber ke akun target terpisah dan untuk memungkinkan kegagalan kembali. Kami tidak menyarankan Anda melampirkan kebijakan ini ke pengguna atau peran IAM Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSElasticDisasterRecoveryStagingAccountPolicy_v2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Januari 2023, 12:11 UTC
- Waktu telah diedit: November 27, 2023, 13:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSStagingAccountPolicyv21",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
        "drs:DescribeJobLogItems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSStagingAccountPolicyv22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/userId" : "${aws:SourceIdentity}"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSStagingAccountPolicyv23",
      "Effect" : "Allow",
      "Action" : "drs:IssueAgentCertificateForDrs",
      "Resource" : [
        "arn:aws:drs:*:*:source-server/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSElasticLoadBalancingClassicServiceRolePolicy

`AWSElasticLoadBalancingClassicServiceRolePolicy`adalah kebijakanAWS terkelola yang: Service Linked Role Policy forAWS Elastic Load Balancing Control Plane - Classic

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini tidak dapat dilampirkan pada pengguna Anda tidak dapat melampirkan kebijakan ini tidak dapat melampirkan kebijakan ini tidak dapat melampirkan

Rincian kebijakan kebijakan kebijakan kebijakan terkait kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 September 2017, 22:36 UTC
- Waktu yang telah diedit: 07 Oktober 2019 23.04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi standar standar kebijakan ini adalah versi terkait izin untuk kebijakan terkait kebijakan terkait kebijakan terkait kebijakan terkait kebijakan terkait kebijakan terkait kebijakan terkait kebijakan terkait kebijakan terkait kebijakan terkait kebijakan terkait kebijakan terkait kebijakan terkait kebijakan terkait kebijakan terkait kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan kebijakan kebijakan kebijakan JSON SON SON SON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterface",
```

```
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSElasticLoadBalancingServiceRolePolicy

`AWSElasticLoadBalancingServiceRolePolicy`adalah kebijakanAWS terkelola yang: Service Linked Role Policy forAWS Elastic Load Balancing Control Plane

Menggunakan kebijakan ini ini yang mengizinkan ini.

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini tidak dapat dilampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 September 2017, 22:19 UTC
- Waktu yang telah diedit: 26 Agustus 2021 19.01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v7 (default)

Versi default kebijakan yang Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan JSON SON SON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:GetCoipPoolUsage",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
```

```
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses",
        "ec2:ReleaseAddress",
        "ec2:UnassignIpv6Addresses",
        "ec2:DescribeVpcPeeringConnections",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "outposts:GetOutpostInstanceTypes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSElementalMediaConvertFullAccess

`AWSElementalMediaConvertFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS Elemental MediaConvert melaluiAWS Management Console dan SDK.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElementalMediaConvertFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 25 Juni 2018, 19:25 UTC
- Waktu yang telah diedit: 10 Juni 2019, 22.52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "mediaconvert.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSElementalMediaConvertReadOnly

`AWSElementalMediaConvertReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja keAWS Elemental MediaConvert melaluiAWS Management Console dan SDK.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElementalMediaConvertReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 25 Juni 2018, 19:25 UTC
- Waktu yang telah diedit: 10 Juni 2019, 22.52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:Get*",
```

```
        "mediaconvert:List*",
        "mediaconvert:DescribeEndpoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSElementalMediaLiveFullAccess

`AWSElementalMediaLiveFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke MediaLive sumber dayaAWS Elemental

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElementalMediaLiveFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 Juli 2020, 17:07 UTC
- Waktu yang telah diedit: 08 Juli 2020, 17.07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "medialive:*",
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSElementalMediaLiveReadOnly

`AWSElementalMediaLiveReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke MediaLive sumber dayaAWS Elemental

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElementalMediaLiveReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 Juli 2020, 16:38 UTC
- Waktu yang telah diedit: 08 Juli 2020, 16.38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "medialive:List*",
      "medialive:Describe*"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSElementalMediaPackageFullAccess

`AWSElementalMediaPackageFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke MediaPackage sumber dayaAWS Elemental

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElementalMediaPackageFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 Desember 2017, 23:39 UTC
- Waktu yang telah diedit: 29 Desember 2017 23.39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackage:*",
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSElementalMediaPackageReadOnly

`AWSElementalMediaPackageReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke MediaPackage sumber dayaAWS Elemental

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElementalMediaPackageReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 Desember 2017, 00:04 UTC
- Waktu yang telah diedit: 30 Desember 2017 09.00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackage:List*",
      "mediapackage:Describe*"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSElementalMediaPackageV2FullAccess

`AWSElementalMediaPackageV2FullAccess`adalahAWSkebijakan terkelolabahwa: Menyediakan akses penuh keAWSElementalMediaPackageSumber daya V2.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElementalMediaPackageV2FullAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 25 Juli 2023, 20:29 UTC
- Waktu yang diedit:25 Juli 2023, 20:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess`

Versi kebijakan

Versi kebijakan: v1(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSElementalMediaPackageV2ReadOnly

`AWSElementalMediaPackageV2ReadOnly`adalahAWSkebijakan terkelolabahwa: Menyediakan akses hanya-baca keAWSElementalMediaPackageSumber daya V2.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElementalMediaPackageV2ReadOnly`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 25 Juli 2023, 20:31 UTC
- Waktu yang diedit:25 Juli 2023, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly`

Versi kebijakan

Versi kebijakan: v1(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai denganAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSElementalMediaStoreFullAccess

`AWSElementalMediaStoreFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca dan tulis lengkap ke semua MediaStore API

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElementalMediaStoreFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 05 Maret 2018, 23:15 UTC
- Waktu yang telah diedit: 05 Maret 2018 05.05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSElementalMediaStoreReadOnly

`AWSElementalMediaStoreReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan izin hanya-baca untuk MediaStore API

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElementalMediaStoreReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 Maret 2018, 19:48 UTC
- Waktu yang telah diedit: 08 Maret 2018 19.48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSElementalMediaTailorFullAccess

`AWSElementalMediaTailorFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke MediaTailor sumber dayaAWS Elemental

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElementalMediaTailorFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 23 November 2021, 00:04 UTC
- Waktu yang telah diedit: 23 November 2021 09.00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediatailor:*",
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSElementalMediaTailorReadOnly

`AWSElementalMediaTailorReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke MediaTailor sumber dayaAWS Elemental

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSElementalMediaTailorReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 23 November 2021, 00:05 UTC
- Waktu yang telah diedit: 23 November 2021 09.00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediatailor:List*",
      "mediatailor:Describe*",
      "mediatailor:Get*"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSEnhancedClassicNetworkingMangementPolicy

`AWSEnhancedClassicNetworkingMangementPolicy`adalah kebijakanAWS terkelola yang: Kebijakan untuk mengaktifkan fitur manajemen jaringan klasik yang disempurnakan.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 September 2017, 17:29 UTC
- Waktu yang telah diedit: 20 September 2017 07.29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSEntityResolutionConsoleFullAccess

`AWSEntityResolutionConsoleFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh konsol ke Resolusi AWS Entitas dan layanan terkait.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSEntityResolutionConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 17 Agustus 2023, 17:54 UTC
- Waktu yang telah diedit: 16 Oktober 2023, 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EntityResolutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "entityresolution:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSourcesConsoleDisplay",
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:GetSchema",
        "glue:SearchTables",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3BucketsConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3SourcesConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListBucketVersions",
        "s3:GetBucketVersioning"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TaggingConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "KMSConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListRolesToPickRoleForPassing",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToEntityResolutionService",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*entityresolution*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "entityresolution.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageEventBridgeRules",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/entity-resolution-automatic*"
      ]
    },
```

```
    {
      "Sid" : "ADXReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:GetDataSet"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSEntityResolutionConsoleReadOnlyAccess

`AWSEntityResolutionConsoleReadOnlyAccess`adalah sebuahAWSkebijakan terkelolaitu: Menyediakan akses hanya-baca keAWSResolusi Entitas melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSEntityResolutionConsoleReadOnlyAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Tipe:AWSkebijakan terkelola
- Waktu pembuatan: 17 Agustus 2023, 18:18 UTC
- Waktu yang diedit:17 Agustus 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1(default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber dayaAWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EntityResolutionRead",
      "Effect" : "Allow",
      "Action" : [
        "entityresolution:Get*",
        "entityresolution:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai denganAWSkebijakan terkelola dan beralih ke izin hak istimewa paling sedikit

AWSFaultInjectionSimulatorEC2Access

`AWSFaultInjectionSimulatorEC2Access`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin Layanan Simulator Injeksi Kesalahan di EC2 dan layanan lain yang diperlukan untuk melakukan tindakan FIS.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFaultInjectionSimulatorEC2Access` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Oktober 2022, 20:39 UTC
- Waktu telah diedit: 27 November 2023, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowEc2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:SendSpotInstanceInterruptions",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "AllowEc2InstancesWithEncryptedEbsVolumes",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSSMSendOnEc2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Sid" : "AllowSSMStopOnEc2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:ListCommands"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSFaultInjectionSimulatorECSAccess

`AWSFaultInjectionSimulatorECSAccess`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin Layanan Simulator Injeksi Kesalahan di ECS dan layanan lain yang diperlukan untuk melakukan tindakan FIS.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFaultInjectionSimulatorECSAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Oktober 2022, 20:37 UTC
- Waktu telah diedit: 25 Januari 2024, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Clusters",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:ListContainerInstances"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "Tasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTasks",
        "ecs:StopTask"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*/*"
      ]
    },
    {
      "Sid" : "ContainerInstances",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateContainerInstancesState"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:container-instance/*/*"
      ]
    },
    {
      "Sid" : "ListTasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTasks"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSend",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Sid" : "SSMList",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSFaultInjectionSimulatorEKSAccess

`AWSFaultInjectionSimulatorEKSAccess`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin Layanan Simulator Injeksi Kesalahan di EKS dan layanan lain yang diperlukan untuk melakukan tindakan FIS.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFaultInjectionSimulatorEKSAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Oktober 2022, 20:34 UTC
- Waktu telah diedit: 13 November 2023, 16:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "DescribeNodeGroup",
      "Effect" : "Allow",
      "Action" : "eks:DescribeNodegroup",
      "Resource" : "arn:aws:eks:*:*:nodegroup/*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSFaultInjectionSimulatorNetworkAccess

`AWSFaultInjectionSimulatorNetworkAccess`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin Layanan Simulator Injeksi Kesalahan di jaringan EC2 dan layanan lain yang diperlukan untuk melakukan tindakan FIS.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFaultInjectionSimulatorNetworkAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Oktober 2022, 20:32 UTC
- Waktu yang telah diedit: 25 Januari 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateTagsOnNetworkAcl",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:CreateAction" : "CreateNetworkAcl",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkAcl",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkAcl",
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteNetworkAcl",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkAclOnVpc",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkAcl",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "VpcActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
```

```
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReplaceNetworkAclAssociation",
      "Effect" : "Allow",
      "Action" : "ec2:ReplaceNetworkAclAssociation",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-acl/*"
      ]
    },
    {
      "Sid" : "GetManagedPrefixListEntries",
      "Effect" : "Allow",
      "Action" : "ec2:GetManagedPrefixListEntries",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*"
    },
    {
      "Sid" : "CreateRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:CreateRouteTable",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRouteTableOnVpc",
      "Effect" : "Allow",
      "Action" : "ec2:CreateRouteTable",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
```

```
    },
    {
      "Sid" : "CreateTagsOnRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateRouteTable",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateManagedPrefixList",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:vpc/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRoute",
      "Effect" : "Allow",
      "Action" : "ec2:CreateRoute",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaceOnSubnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "DeleteNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateManagedPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:CreateManagedPrefixList",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteManagedPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteManagedPrefixList",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyManagedPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:ModifyManagedPrefixList",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "ReplaceRouteTableAssociation",
      "Effect" : "Allow",
      "Action" : "ec2:ReplaceRouteTableAssociation",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
```

```
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "AssociateRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:AssociateRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "DisassociateRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:DisassociateRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DisassociateRouteTableOnSubnet",
      "Effect" : "Allow",
      "Action" : "ec2:DisassociateRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "ModifyVpcEndpointOnRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:ModifyVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "ModifyVpcEndpoint",
      "Effect" : "Allow",
      "Action" : "ec2:ModifyVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ]
    },
    {
      "Sid" : "TransitGatewayRouteTableAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:AssociateTransitGatewayRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSFaultInjectionSimulatorRDSAccess

`AWSFaultInjectionSimulatorRDSAccess`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin Layanan Simulator Injeksi Kesalahan di RDS dan layanan lain yang diperlukan untuk melakukan tindakan FIS.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFaultInjectionSimulatorRDSAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Oktober 2022, 20:30 UTC
- Waktu telah diedit: 13 November 2023, 16:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFailover",
      "Effect" : "Allow",
      "Action" : [
        "rds:FailoverDBCluster"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "AllowReboot",
```

```
      "Effect" : "Allow",
      "Action" : [
        "rds:RebootDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*"
      ]
    },
    {
      "Sid" : "DescribeResources",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSFaultInjectionSimulatorSSMAccess

`AWSFaultInjectionSimulatorSSMAccess`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin Layanan Simulator Injeksi Kesalahan di SSM dan layanan lain yang diperlukan untuk melakukan tindakan FIS.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSFaultInjectionSimulatorSSMAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 Oktober 2022, 15:33 UTC
- Waktu yang telah diedit: 02 Juni 2023, 22.55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSFinSpaceServiceRolePolicy

`AWSFinSpaceServiceRolePolicy`adalah kebijakan AWS terkelola yang: Kebijakan untuk mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon FinSpace

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Mei 2023, 16:42 UTC
- Waktu yang telah diedit: 01 Desember 2023, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSFinSpaceServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
```

```
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/FinSpace",
            "AWS/Usage"
          ]
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSFMAdminFullAccess

`AWSFMAdminFullAccess`adalah kebijakanAWS terkelola yang: Akses penuh untuk AdministratorAWS FM

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSFMAdminFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 Mei 2018, 18:06 UTC
- Waktu yang telah diedit: 20 Oktober 2022, 23.39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fms:*",
        "waf:*",
        "waf-regional:*",
        "elasticloadbalancing:SetWebACL",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "shield:GetSubscriptionState",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:CheckCapacity",
        "wafv2:PutLoggingConfiguration",
        "wafv2:ListAvailableManagedRuleGroupVersions",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:ListRuleGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fms.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListDelegatedAdministrators",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "fms.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSFMAdminReadOnlyAccess

`AWSFMAdminReadOnlyAccess`adalah kebijakanAWS terkelola yang: Baca hanya akses untuk AdministratorAWS FM yang memungkinkan pemantauan operasiAWS FM

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSFMAdminReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 Mei 2018, 20:07 UTC
- Waktu yang telah diedit: 31 Oktober 2022, 22.42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fms:Get*",
        "fms:List*",
        "waf:Get*",
        "waf:List*",
```

```
        "waf-regional:Get*",
        "waf-regional:List*",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "shield:GetSubscriptionState",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:CheckCapacity",
        "wafv2:ListAvailableManagedRuleGroupVersions",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:ListRuleGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "fms.amazonaws.com"
```

```
            ]
          }
        }
      }
    ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSFMMemberReadOnlyAccess

`AWSFMMemberReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke tindakanAWS WAF untuk akun anggotaAWS Firewall Manager

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSFMMemberReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 Mei 2018, 21:05 UTC
- Waktu yang telah diedit: 09 Mei 2018 09.05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSForWordPressPluginPolicy

`AWSForWordPressPluginPolicy`adalah kebijakanAWS terkelola yang: Kebijakan terkelola untukAWS Untuk Plugin Wordpress

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSForWordPressPluginPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 Oktober 2019, 00:27 UTC
- Waktu yang telah diedit: 20 Januari 2020, 23.20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Permissions1",
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech",
        "polly:DescribeVoices",
        "translate:TranslateText"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Permissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:CreateBucket",
```

```
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::audio_for_wordpress*",
        "arn:aws:s3:::audio-for-wordpress*"
      ]
    },
    {
      "Sid" : "Permissions3",
      "Effect" : "Allow",
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:DescribeCertificate",
        "acm:RequestCertificate",
        "cloudformation:CreateStack",
        "cloudfront:ListDistributions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "us-east-1"
        }
      }
    },
    {
      "Sid" : "Permissions4",
      "Effect" : "Allow",
      "Action" : [
        "acm:DeleteCertificate",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:UpdateStack",
        "cloudfront:CreateDistribution",
        "cloudfront:CreateInvalidation",
        "cloudfront:DeleteDistribution",
        "cloudfront:GetDistribution",
        "cloudfront:GetInvalidation",
        "cloudfront:TagResource",
        "cloudfront:UpdateDistribution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/createdBy" : "AWSForWordPressPlugin"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSGitSyncServiceRolePolicy

`AWSGitSyncServiceRolePolicy`adalah kebijakan AWS terkelola yang: Kebijakan yang memungkinkan Koneksi AWS Kode menyinkronkan konten dari repositori git Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 16 November 2023, 17:05 UTC
- Waktu telah diedit: 16 November 2023, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGlobalAcceleratorSLRPolicy

`AWSGlobalAcceleratorSLRPolicy`adalah kebijakan AWS terkelola yang: Kebijakan memberikan izin kepada AWS Global Accelerator untuk mengelola Antarmuka Jaringan Elastis EC2 dan Grup Keamanan.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 April 2019, 19:39 UTC
- Waktu telah diedit: September 12, 2023, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Action1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAddresses"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSServiceName" : "GlobalAccelerator"
        }
      }
    },
    {
      "Sid" : "EC2Action3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElbAction1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action4",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
```

```
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGlueConsoleFullAccess

`AWSGlueConsoleFullAccess`adalahAWSkebijakan terkelolabahwa: Menyediakan akses penuh keAWSLem melaluiAWS Management Console

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSGlueConsoleFullAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 14 Agustus 2017, 13:37 UTC
- Waktu yang diedit:14 Juli 2023, 14:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v14(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "BaseAppPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBSubnetGroups",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplateSummary",
        "dynamodb:ListTables",
        "kms:ListAliases",
        "kms:DescribeKey",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListDashboards",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:DescribeRecipe"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*",
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
        },
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ZeppelinInstance"
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSGlueServiceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai denganAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSGlueConsoleSageMakerNotebookFullAccess

`AWSGlueConsoleSageMakerNotebookFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS Glue melaluiAWS Management Console dan akses ke instance notebook sagemaker.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSGlueConsoleSageMakerNotebookFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 05 Oktober 2018, 17:52 UTC
- Waktu yang telah diedit: 15 Juli 2021 15.24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:CreateNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "rds:DescribeDBInstances",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplateSummary",
        "dynamodb:ListTables",
        "kms:ListAliases",
        "kms:DescribeKey",
        "sagemaker:ListNotebookInstances",
        "cloudformation:ListStacks",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListDashboards"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*aws-glue-*/*",
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedNotebookInstanceUrl",
```

```
        "sagemaker:CreateNotebookInstance",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StopNotebookInstance",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:ListTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance/aws-glue-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:ListNotebookInstanceLifecycleConfigs"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/aws-glue-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
        },
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ZeppelinInstance"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "aws-glue-*"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceSageMakerNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSGlueServiceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AwsGlueDataBrewFullAccessPolicy

`AwsGlueDataBrewFullAccessPolicy`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS Glue DataBrew melaluiAWS Management Console. Juga menyediakan akses pilih ke layanan terkait (misalnya, S3, KMS, Glue).

Menggunakan kebijakan ini

Anda dapat melampirkan`AwsGlueDataBrewFullAccessPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 November 2020, 16:51 UTC
- Waktu yang telah diedit: 04 Pebruari 2022, 18.28 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy`

Versi kebijakan

Versi kebijakan:v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "databrew:CreateDataset",
        "databrew:DescribeDataset",
        "databrew:ListDatasets",
        "databrew:UpdateDataset",
        "databrew:DeleteDataset",
        "databrew:CreateProject",
        "databrew:DescribeProject",
        "databrew:ListProjects",
        "databrew:StartProjectSession",
        "databrew:SendProjectSessionAction",
        "databrew:UpdateProject",
        "databrew:DeleteProject",
        "databrew:CreateRecipe",
        "databrew:DescribeRecipe",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:PublishRecipe",
        "databrew:UpdateRecipe",
        "databrew:BatchDeleteRecipeVersion",
        "databrew:DeleteRecipeVersion",
        "databrew:CreateRecipeJob",
        "databrew:CreateProfileJob",
        "databrew:DescribeJob",
        "databrew:DescribeJobRun",
        "databrew:ListJobRuns",
        "databrew:ListJobs",
        "databrew:StartJobRun",
        "databrew:StopJobRun",
        "databrew:UpdateProfileJob",
        "databrew:UpdateRecipeJob",
        "databrew:DeleteJob",
        "databrew:CreateSchedule",
        "databrew:DescribeSchedule",
        "databrew:ListSchedules",
        "databrew:UpdateSchedule",
```

```
        "databrew:DeleteSchedule",
        "databrew:CreateRuleset",
        "databrew:DeleteRuleset",
        "databrew:DescribeRuleset",
        "databrew:ListRulesets",
        "databrew:UpdateRuleset",
        "databrew:ListTagsForResource",
        "databrew:TagResource",
        "databrew:UntagResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:ListFlows",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetDataCatalogEncryptionSettings",
        "dataexchange:ListDataSets",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:ListRevisionAssets",
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:GetJob",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
```

```
        "redshift-data:ListTables",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "secretsmanager:ListSecrets",
        "secretsmanager:DescribeSecret",
        "sts:GetCallerIdentity",
        "cloudtrail:LookupEvents",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/AwsGlueDataBrew-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
```

```
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*/awsgluedatabrew*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::databrew-public-datasets-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AwsGlueDataBrew-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateRandom"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "databrew.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "databrew!default"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "databrew.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "databrew.amazonaws.com"
          ]
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSGlueDataBrewServiceRole

`AWSGlueDataBrewServiceRole`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin untuk merekatkan untuk melakukan tindakan pada katalog data lem pengguna, kebijakan ini juga memberikan izin untuk tindakan ec2 untuk memungkinkan lem membuat ENI terhubung ke sumber daya di VPC, juga memungkinkan lem untuk mengakses data terdaftar di lakeformation dan izin untuk mengakses cloudwatch pengguna

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGlueDataBrewServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 04 Desember 2020, 21:26 UTC
- Waktu telah diedit: 20 Maret 2024, 23:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetConnection"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "GluePIIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGetCustomEntityTypes",
        "glue:GetCustomEntityType"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3PublicDatasetAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::databrew-public-datasets-*"
      ]
    },
    {
      "Sid" : "EC2NetworkingPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2DeleteGlueNetworkInterfacePermissions",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws-glue-service-resource" : "*"
        }
      },
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2GlueTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
```

```
      ]
    },
    {
      "Sid" : "GlueDatabrewLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws-glue-databrew/*"
      ]
    },
    {
      "Sid" : "LakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGlueSchemaRegistryFullAccess

`AWSGlueSchemaRegistryFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Layanan Registri SkemaAWS Glue

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSGlueSchemaRegistryFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 20 November 2020, 00:19 UTC
- Waktu yang telah diedit: 20 November 2020, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGlueSchemaRegistryFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateRegistry",
        "glue:UpdateRegistry",
        "glue:DeleteRegistry",
        "glue:GetRegistry",
        "glue:ListRegistries",
```

```
        "glue:CreateSchema",
        "glue:UpdateSchema",
        "glue:DeleteSchema",
        "glue:GetSchema",
        "glue:ListSchemas",
        "glue:RegisterSchemaVersion",
        "glue:DeleteSchemaVersions",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:ListSchemaVersions",
        "glue:CheckSchemaVersionValidity",
        "glue:PutSchemaVersionMetadata",
        "glue:RemoveSchemaVersionMetadata",
        "glue:QuerySchemaVersionMetadata"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSGlueSchemaRegistryTagsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTags",
        "glue:TagResource",
        "glue:UnTagResource"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:schema/*",
        "arn:aws:glue:*:*:registry/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSGlueSchemaRegistryReadonlyAccess

`AWSGlueSchemaRegistryReadonlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses readonly ke Layanan RegistryAWS Glue Schema

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSGlueSchemaRegistryReadonlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 20 November 2020, 00:20 UTC
- Waktu yang telah diedit: 20 November 2020, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadonlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGlueSchemaRegistryReadonlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetRegistry",
        "glue:ListRegistries",
        "glue:GetSchema",
        "glue:ListSchemas",
```

```
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:ListSchemaVersions",
        "glue:GetSchemaVersionsDiff",
        "glue:CheckSchemaVersionValidity",
        "glue:QuerySchemaVersionMetadata",
        "glue:GetTags"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSGlueServiceNotebookRole

`AWSGlueServiceNotebookRole`adalah kebijakan AWS terkelola yang: Kebijakan untuk peran layanan AWS Glue yang memungkinkan pelanggan mengelola server notebook

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGlueServiceNotebookRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Agustus 2017, 13:37 UTC
- Waktu telah diedit: 09 Oktober 2023, 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:DeleteDatabase",
        "glue:DeletePartition",
        "glue:DeleteTable",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:CreateConnection",
        "glue:CreateJob",
        "glue:DeleteConnection",
        "glue:DeleteJob",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:UpdateJob",
```

```
        "glue:BatchDeleteConnection",
        "glue:UpdateConnection",
        "glue:GetUserDefinedFunction",
        "glue:UpdateUserDefinedFunction",
        "glue:GetUserDefinedFunctions",
        "glue:DeleteUserDefinedFunction",
        "glue:CreateUserDefinedFunction",
        "glue:BatchGetPartition",
        "glue:BatchDeletePartition",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteTable",
        "glue:UpdateDevEndpoint",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*",
        "arn:aws:s3:::aws-glue*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGlueServiceRole

`AWSGlueServiceRole`adalah kebijakan AWS terkelola yang: Kebijakan untuk peran layanan AWS Glue yang memungkinkan akses ke layanan terkait termasuk EC2, S3, dan Cloudwatch Logs

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGlueServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Agustus 2017, 13:37 UTC

- Waktu telah diedit: September 11, 2023, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*",
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AwsGlueSessionUserRestrictedNotebookPolicy

`AwsGlueSessionUserRestrictedNotebookPolicy`adalah kebijakan AWS terkelola yang: Menyediakan izin yang memungkinkan pengguna membuat dan hanya menggunakan sesi buku catatan yang terkait dengan pengguna. Kebijakan ini juga mencakup izin untuk secara eksplisit mengizinkan pengguna melewati peran sesi Glue terbatas.

Menggunakan kebijakan ini

Anda dapat melampirkan `AwsGlueSessionUserRestrictedNotebookPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 18 April 2022, 15:24 UTC
- Waktu telah diedit: 22 November 2023, 01:32 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NotebokAllowActions0",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "NotebookAllowActions1",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "NotebookAllowActions2",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Sid" : "NotebookAllowActions3",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "NotebookDenyActions",
```

```
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "NotebookPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AwsGlueSessionServiceRoleUserRestrictedForNotebook*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AwsGlueSessionUserRestrictedNotebookServiceRole

`AwsGlueSessionUserRestrictedNotebookServiceRole`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke semua sumber dayaAWS Glue kecuali untuk sesi. Memungkinkan pengguna untuk membuat dan menggunakan hanya sesi notebook yang terkait dengan pengguna. Kebijakan ini juga mencakup izin lain yang diperlukan olehAWS Glue untuk mengelola sumber daya Glue diAWS layanan lain.

Menggunakan kebijakan ini

Anda dapat melampirkan`AwsGlueSessionUserRestrictedNotebookServiceRole` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 18 April 2022, 15:27 UTC
- Waktu yang telah diedit: 18 April 2022, 15.27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
```

```
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
```

```
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AwsGlueSessionUserRestrictedPolicy

`AwsGlueSessionUserRestrictedPolicy`adalah kebijakanAWS terkelola yang: Menyediakan izin yang memungkinkan pengguna untuk membuat dan menggunakan hanya sesi interaktif yang terkait dengan pengguna. Kebijakan ini juga mencakup izin untuk secara eksplisit mengizinkan pengguna meneruskan peran sesi Glue yang dibatasi.

Menggunakan kebijakan ini

Anda dapat melampirkan`AwsGlueSessionUserRestrictedPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 14 April 2022, 21:31 UTC
- Waktu yang telah diedit: 14 April 2022, 21.31 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AwsGlueSessionServiceRoleUserRestricted*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AwsGlueSessionUserRestrictedServiceRole

`AwsGlueSessionUserRestrictedServiceRole`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke semua sumber dayaAWS Glue kecuali untuk sesi. Memungkinkan pengguna untuk membuat dan menggunakan hanya sesi interaktif yang terkait dengan pengguna. Kebijakan ini juga mencakup izin lain yang diperlukan olehAWS Glue untuk mengelola sumber daya Glue diAWS layanan lain

Menggunakan kebijakan ini

Anda dapat melampirkan`AwsGlueSessionUserRestrictedServiceRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 April 2022, 21:30 UTC
- Waktu yang telah diedit: 14 April 2022, 21.30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
```

```
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSGrafanaAccountAdministrator

`AWSGrafanaAccountAdministrator`adalah kebijakanAWS terkelola yang: Menyediakan akses dalam Amazon Grafana untuk membuat dan mengelola ruang kerja untuk seluruh organisasi.

Menggunakan kebijakan

Anda dapat melampirkan`AWSGrafanaAccountAdministrator` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 23 Februari 2021, 00:20 UTC
- Waktu yang telah diedit: 15 Februari 2022, 22.36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaOrganizationAdmin",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaIAMGetRolePermission",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaIAMPassRolePermission",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "grafana.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSGrafanaConsoleReadOnlyAccess

`AWSGrafanaConsoleReadOnlyAccess`adalah kebijakanAWS terkelola yang: Akses ke operasi baca saja di Amazon Grafana.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSGrafanaConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 23 Februari 2021, 00:10 UTC
- Waktu yang telah diedit: 15 Februari 2022, 22.30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AWSGrafanaConsoleReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:Describe*",
        "grafana:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSGrafanaWorkspacePermissionManagement

`AWSGrafanaWorkspacePermissionManagement`adalah kebijakanAWS terkelola yang: Hanya menyediakan kemampuan untuk memperbarui izin pengguna dan grup untuk ruang kerjaAWS Grafana.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSGrafanaWorkspacePermissionManagement` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 23 Februari 2021, 00:15 UTC
- Waktu yang diedit: 15 Maret 2023, 22.17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:UpdatePermissions",
        "grafana:ListPermissions",
        "grafana:ListWorkspaces"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces*"
    },
    {
      "Sid" : "IAMIdentityCenterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:ListDirectoryAssociations",
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso-directory:DescribeUser",
        "sso-directory:DescribeGroup"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSGrafanaWorkspacePermissionManagementV2

`AWSGrafanaWorkspacePermissionManagementV2`adalah kebijakan AWS terkelola yang: Menyediakan kemampuan untuk memperbarui izin pengguna dan grup IAM Identity Center (IDC) untuk ruang kerja Grafana yang Dikelola Amazon.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSGrafanaWorkspacePermissionManagementV2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Januari 2024, 18:39 UTC
- Waktu telah diedit: 05 Januari 2024, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:UpdatePermissions",
        "grafana:ListPermissions",
        "grafana:ListWorkspaces"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces*"
    },
    {
      "Sid" : "IAMIdentityCenterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:ListDirectoryAssociations",
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso-directory:DescribeUser",
        "sso-directory:DescribeGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSGreengrassFullAccess

`AWSGreengrassFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan akses penuh ke konfigurasiAWS Greengrass, manajemen, dan tindakan penyebaran

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSGreengrassFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 Mei 2017, 00:47 UTC
- Waktu yang telah diedit: 03 Mei 2017 01.47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "greengrass:*"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSGreengrassReadOnlyAccess

`AWSGreengrassReadOnlyAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan akses hanya baca ke konfigurasiAWS Greengrass, manajemen, dan tindakan penyebaran

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSGreengrassReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 Oktober 2018, 16:01 UTC
- Waktu yang telah diedit: 30 Oktober 2018 16.01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "greengrass:List*",
        "greengrass:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSGreengrassResourceAccessRolePolicy

`AWSGreengrassResourceAccessRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan untuk peran layananAWS Greengrass yang memungkinkan akses ke layanan terkait termasukAWS Lambda danAWS IoT thing shadow.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSGreengrassResourceAccessRolePolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Februari 2017, 21:17 UTC
- Waktu yang telah diedit: 14 November 2018, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGreengrassAccessToShadows",
      "Action" : [
        "iot:DeleteThingShadow",
        "iot:GetThingShadow",
        "iot:UpdateThingShadow"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iot:*:*:thing/GG_*",
        "arn:aws:iot:*:*:thing/*-gcm",
        "arn:aws:iot:*:*:thing/*-gda",
        "arn:aws:iot:*:*:thing/*-gci"
      ]
    },
    {
      "Sid" : "AllowGreengrassToDescribeThings",
      "Action" : [
        "iot:DescribeThing"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iot:*:*:thing/*"
    },
    {
      "Sid" : "AllowGreengrassToDescribeCertificates",
      "Action" : [
        "iot:DescribeCertificate"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iot:*:*:cert/*"
```

```
    },
    {
      "Sid" : "AllowGreengrassToCallGreengrassServices",
      "Action" : [
        "greengrass:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGreengrassToGetLambdaFunctions",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGreengrassToGetGreengrassSecrets",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
    },
    {
      "Sid" : "AllowGreengrassAccessToS3Objects",
      "Action" : [
        "s3:GetObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::*Greengrass*",
        "arn:aws:s3:::*GreenGrass*",
        "arn:aws:s3:::*greengrass*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowGreengrassAccessToS3BucketLocation",
      "Action" : [
```

```
        "s3:GetBucketLocation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGreengrassAccessToSageMakerTrainingJobs",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSGroundStationAgentInstancePolicy

`AWSGroundStationAgentInstancePolicy`adalah kebijakanAWS terkelola yang: Menyediakan izin Instans Titik Akhir Dataflow untuk menggunakan AgenAWS Ground Station

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSGroundStationAgentInstancePolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 Maret 2023, 15:23 UTC

- Waktu yang telah diedit: 29 Maret 2023, 15.23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "groundstation:RegisterAgent",
        "groundstation:UpdateAgentStatus",
        "groundstation:GetAgentConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSHealth_EventProcessorServiceRolePolicy

`AWSHealth_EventProcessorServiceRolePolicy`adalah kebijakanAWS terkelola yang: MemungkinkanAWS Health untuk mengaktifkan fitur prosesor acara Health.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 Januari 2023, 19:24 UTC
- Waktu yang telah diedit: 13 Januari 2023, 19.24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule",
        "events:RemoveTargets"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "event-processor.health.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSHealthFullAccess

`AWSHealthFullAccess`adalah kebijakanAWS terkelola yang: Memungkinkan akses penuh ke API dan Pemberitahuan dan Personal Health DashboardAWS

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSHealthFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Desember 2016, 12:30 UTC
- Waktu yang telah diedit: 16 November 2020 08.08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthFullAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "health.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "health:*",
        "organizations:ListAccounts",
        "organizations:ListParents",
        "organizations:DescribeAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "health.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSHealthImagingFullAccess

`AWSHealthImagingFullAccess`adalahAWSkebijakan terkelolabahwa: Menyediakan akses penuh keAWSLayanan Pencitraan Kesehatan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSHealthImagingFullAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 25 Juli 2023, 23:39 UTC
- Waktu yang diedit:25 Juli 2023, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingFullAccess`

Versi kebijakan

Versi kebijakan: v1(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "medical-imaging:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "medical-imaging.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSHealthImagingReadOnlyAccess

`AWSHealthImagingReadOnlyAccess`adalah sebuahAWSkebijakan terkelolabahwa: Menyediakan akses hanya baca keAWSLayanan Pencitraan Kesehatan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSHealthImagingReadOnlyAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 25 Juli 2023, 23:40 UTC
- Waktu yang diedit:01 Agustus 2023, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2(default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "medical-imaging:GetDICOMImportJob",
        "medical-imaging:GetDatastore",
        "medical-imaging:GetImageFrame",
        "medical-imaging:GetImageSet",
        "medical-imaging:GetImageSetMetadata",
        "medical-imaging:ListDICOMImportJobs",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListImageSetVersions",
        "medical-imaging:ListTagsForResource",
        "medical-imaging:SearchImageSets"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai denganAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIAMIdentityCenterAllowListForIdentityContext

`AWSIAMIdentityCenterAllowListForIdentityContext`adalah kebijakan AWS terkelola yang: Menyediakan daftar tindakan yang diizinkan untuk peran yang diambil dengan konteks identitas Pusat Identitas IAM. AWS Security Token Service (AWSSTS) secara otomatis melampirkan kebijakan ini ke peran yang diasumsikan. Konteks identitas diteruskan sebagai ProvidedContext.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIAMIdentityCenterAllowListForIdentityContext` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 08 November 2023, 15:21 UTC
- Waktu telah diedit: November 25, 2023, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedIdentityPropagation",
      "Effect" : "Deny",
      "NotAction" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreatePreparedStatement",
        "athena:DeleteNamedQuery",
        "athena:DeletePreparedStatement",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:UpdateNamedQuery",
        "athena:UpdatePreparedStatement",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups",
        "elasticmapreduce:GetClusterSessionCredentials",
        "glue:GetDatabase",
```

```
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersions",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:SearchTables",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchUpdatePartition",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "lakeformation:GetDataAccess",
        "s3:GetAccessGrantsInstanceForPrefix",
        "s3:GetDataAccess"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIdentitySyncFullAccess

`AWSIdentitySyncFullAccess`adalah kebijakanAWS terkelola yang: Memberikan akses penuh ke layanan Identity Sync

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIdentitySyncFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 23 Maret 2022, 23:29 UTC
- Waktu yang telah diedit: 23 Maret 2022, 23.29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication"
      ],
      "Resource" : "arn:*:ds:*:*:*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "identity-sync:DeleteSyncProfile",
        "identity-sync:CreateSyncProfile",
        "identity-sync:GetSyncProfile",
        "identity-sync:StartSync",
        "identity-sync:StopSync",
        "identity-sync:CreateSyncFilter",
        "identity-sync:DeleteSyncFilter",
        "identity-sync:ListSyncFilters",
        "identity-sync:CreateSyncTarget",
        "identity-sync:DeleteSyncTarget",
        "identity-sync:GetSyncTarget",
        "identity-sync:UpdateSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIdentitySyncReadOnlyAccess

`AWSIdentitySyncReadOnlyAccess`adalah kebijakanAWS terkelola yang: Hanya baca akses ke layanan Identity Sync

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIdentitySyncReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 23 Maret 2022, 23:29 UTC

- Waktu yang telah diedit: 23 Maret 2022, 23.29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSImageBuilderFullAccess

`AWSImageBuilderFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke semua tindakanAWS Image Builder dan akses scoped sumber daya keAWS layanan terkait.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSImageBuilderFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 20 Desember 2019, 18:25 UTC
- Waktu yang telah diedit: 13 April 2021 17.33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:*imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListLicenseSpecificationsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/*imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*imagebuilder*",
        "arn:aws:iam::*:role/*imagebuilder*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3::*:*imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "imagebuilder.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeVolumes",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSImageBuilderReadOnlyAccess

`AWSImageBuilderReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke semua tindakanAWS Image Builder.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSImageBuilderReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 19 Desember 2019, 22:29 UTC
- Waktu yang telah diedit: 19 Desember 2019 08.29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:Get*",
        "imagebuilder:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSImportExportFullAccess

`AWSImportExportFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca dan tulis ke pekerjaan yang dibuat di bawahAkun AWS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSImportExportFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 08.40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "importexport:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSImportExportReadOnlyAccess

`AWSImportExportReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke pekerjaan yang dibuat di bawahAkun AWS.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSImportExportReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 08.40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "importexport:ListJobs",
        "importexport:GetStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIncidentManagerIncidentAccessServiceRolePolicy

`AWSIncidentManagerIncidentAccessServiceRolePolicy`adalah kebijakan AWS terkelola yang: Memberikan izin Manajer Insiden untuk memanggil AWS layanan lain sebagai bagian dari pengelolaan insiden.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSIncidentManagerIncidentAccessServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 November 2023, 00:01 UTC
- Waktu telah diedit: 20 Februari 2024, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIncidentManagerResolverAccess

`AWSIncidentManagerResolverAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin untuk memulai, melihat, dan memperbarui insiden dengan akses penuh ke peristiwa timeline kustom & item terkait. Tetapkan kebijakan ini kepada pengguna yang akan membuat dan menyelesaikan insiden.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIncidentManagerResolverAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 10 Mei 2021, 06:12 UTC
- Waktu yang telah diedit: 10 Mei 2021 06.12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:StartIncident"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResponsePlanReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:GetResponsePlan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentRecordResolverPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:UpdateIncidentRecord",
        "ssm-incidents:ListTimelineEvents",
        "ssm-incidents:CreateTimelineEvent",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:UpdateTimelineEvent",
        "ssm-incidents:DeleteTimelineEvent",
        "ssm-incidents:ListRelatedItems",
        "ssm-incidents:UpdateRelatedItems"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIncidentManagerServiceRolePolicy

`AWSIncidentManagerServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin kepada Manajer Insiden untuk mengelola catatan insiden dan sumber daya terkait atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, pengguna, pengguna,, pengguna,, pengguna,,, pengguna,, pengguna,, pengguna,,

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Mei 2021, 03:34 UTC
- Waktu yang telah diedit: 05 Desember 2022, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UpdateIncidentRecordPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:CreateTimelineEvent"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedOpsItemPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AssociateOpsItemRelatedItem"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentEngagementPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-contacts:StartEngagement",
      "Resource" : "*"
    },
    {
      "Sid" : "PutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/IncidentManager"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoT1ClickFullAccess

`AWSIoT1ClickFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS IoT 1-Click.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoT1ClickFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Mei 2018, 22:10 UTC
- Waktu yang telah diedit: 11 Mei 2018 07.10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoT1ClickReadOnlyAccess

`AWSIoT1ClickReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja keAWS IoT 1-Click.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoT1ClickReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Mei 2018, 21:49 UTC
- Waktu yang telah diedit: 11 Mei 2018 09.50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoTAnalyticsFullAccess

`AWSIoTAnalyticsFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke IoT Analytics.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTAnalyticsFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 18 Juni 2018, 23:02 UTC
- Waktu yang telah diedit: 18 Juni 2018, 23.02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotanalytics:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoTAnalyticsReadOnlyAccess

`AWSIoTAnalyticsReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke IoT Analytics.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTAnalyticsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 18 Juni 2018, 21:37 UTC
- Waktu yang telah diedit: 18 Juni 2018 09.37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotanalytics:Describe*",
        "iotanalytics:List*",
        "iotanalytics:Get*",
        "iotanalytics:SampleChannelData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoTConfigAccess

`AWSIoTConfigAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan akses penuh ke tindakan konfigurasiAWS IoT

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTConfigAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Oktober 2015, 21:52 UTC
- Waktu yang telah diedit: 27 September 2019 20.48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigAccess`

Versi kebijakan

Versi kebijakan:v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:AcceptCertificateTransfer",
        "iot:AddThingToThingGroup",
        "iot:AssociateTargetsWithJob",
        "iot:AttachPolicy",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CancelCertificateTransfer",
        "iot:CancelJob",
```

```
        "iot:CancelJobExecution",
        "iot:ClearDefaultAuthorizer",
        "iot:CreateAuthorizer",
        "iot:CreateCertificateFromCsr",
        "iot:CreateJob",
        "iot:CreateKeysAndCertificate",
        "iot:CreateOTAUpdate",
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion",
        "iot:CreateRoleAlias",
        "iot:CreateStream",
        "iot:CreateThing",
        "iot:CreateThingGroup",
        "iot:CreateThingType",
        "iot:CreateTopicRule",
        "iot:DeleteAuthorizer",
        "iot:DeleteCACertificate",
        "iot:DeleteCertificate",
        "iot:DeleteJob",
        "iot:DeleteJobExecution",
        "iot:DeleteOTAUpdate",
        "iot:DeletePolicy",
        "iot:DeletePolicyVersion",
        "iot:DeleteRegistrationCode",
        "iot:DeleteRoleAlias",
        "iot:DeleteStream",
        "iot:DeleteThing",
        "iot:DeleteThingGroup",
        "iot:DeleteThingType",
        "iot:DeleteTopicRule",
        "iot:DeleteV2LoggingLevel",
        "iot:DeprecateThingType",
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeDefaultAuthorizer",
        "iot:DescribeEndpoint",
        "iot:DescribeEventConfigurations",
        "iot:DescribeIndex",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DescribeRoleAlias",
        "iot:DescribeStream",
        "iot:DescribeThing",
```

```
        "iot:DescribeThingGroup",
        "iot:DescribeThingRegistrationTask",
        "iot:DescribeThingType",
        "iot:DetachPolicy",
        "iot:DetachPrincipalPolicy",
        "iot:DetachThingPrincipal",
        "iot:DisableTopicRule",
        "iot:EnableTopicRule",
        "iot:GetEffectivePolicies",
        "iot:GetIndexingConfiguration",
        "iot:GetJobDocument",
        "iot:GetLoggingOptions",
        "iot:GetOTAUpdate",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:GetRegistrationCode",
        "iot:GetTopicRule",
        "iot:GetV2LoggingOptions",
        "iot:ListAttachedPolicies",
        "iot:ListAuthorizers",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCertificatesByCA",
        "iot:ListIndices",
        "iot:ListJobExecutionsForJob",
        "iot:ListJobExecutionsForThing",
        "iot:ListJobs",
        "iot:ListOTAUpdates",
        "iot:ListOutgoingCertificates",
        "iot:ListPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPolicyVersions",
        "iot:ListPrincipalPolicies",
        "iot:ListPrincipalThings",
        "iot:ListRoleAliases",
        "iot:ListStreams",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroups",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:ListThingRegistrationTaskReports",
        "iot:ListThingRegistrationTasks",
        "iot:ListThings",
        "iot:ListThingsInThingGroup",
```

```
        "iot:ListThingTypes",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:RegisterCACertificate",
        "iot:RegisterCertificate",
        "iot:RegisterThing",
        "iot:RejectCertificateTransfer",
        "iot:RemoveThingFromThingGroup",
        "iot:ReplaceTopicRule",
        "iot:SearchIndex",
        "iot:SetDefaultAuthorizer",
        "iot:SetDefaultPolicyVersion",
        "iot:SetLoggingOptions",
        "iot:SetV2LoggingLevel",
        "iot:SetV2LoggingOptions",
        "iot:StartThingRegistrationTask",
        "iot:StopThingRegistrationTask",
        "iot:TestAuthorization",
        "iot:TestInvokeAuthorizer",
        "iot:TransferCertificate",
        "iot:UpdateAuthorizer",
        "iot:UpdateCACertificate",
        "iot:UpdateCertificate",
        "iot:UpdateEventConfigurations",
        "iot:UpdateIndexingConfiguration",
        "iot:UpdateRoleAlias",
        "iot:UpdateStream",
        "iot:UpdateThing",
        "iot:UpdateThingGroup",
        "iot:UpdateThingGroupsForThing",
        "iot:UpdateAccountAuditConfiguration",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DeleteAccountAuditConfiguration",
        "iot:StartOnDemandAuditTask",
        "iot:CancelAuditTask",
        "iot:DescribeAuditTask",
        "iot:ListAuditTasks",
        "iot:CreateScheduledAudit",
        "iot:UpdateScheduledAudit",
        "iot:DeleteScheduledAudit",
        "iot:DescribeScheduledAudit",
        "iot:ListScheduledAudits",
        "iot:ListAuditFindings",
        "iot:CreateSecurityProfile",
```

```
        "iot:DescribeSecurityProfile",
        "iot:UpdateSecurityProfile",
        "iot:DeleteSecurityProfile",
        "iot:AttachSecurityProfile",
        "iot:DetachSecurityProfile",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListActiveViolations",
        "iot:ListViolationEvents",
        "iot:ValidateSecurityProfileBehaviors"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin izin izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoTConfigReadOnlyAccess

`AWSIoTConfigReadOnlyAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan akses hanya baca ke tindakan konfigurasiAWS IoT

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTConfigReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Oktober 2015, 21:52 UTC
- Waktu yang telah diedit: 27 September 2019 20.52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeDefaultAuthorizer",
        "iot:DescribeEndpoint",
        "iot:DescribeEventConfigurations",
        "iot:DescribeIndex",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DescribeRoleAlias",
        "iot:DescribeStream",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingRegistrationTask",
        "iot:DescribeThingType",
        "iot:GetEffectivePolicies",
        "iot:GetIndexingConfiguration",
        "iot:GetJobDocument",
        "iot:GetLoggingOptions",
        "iot:GetOTAUpdate",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:GetRegistrationCode",
        "iot:GetTopicRule",
        "iot:GetV2LoggingOptions",
        "iot:ListAttachedPolicies",
        "iot:ListAuthorizers",
```

```
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCertificatesByCA",
        "iot:ListIndices",
        "iot:ListJobExecutionsForJob",
        "iot:ListJobExecutionsForThing",
        "iot:ListJobs",
        "iot:ListOTAUpdates",
        "iot:ListOutgoingCertificates",
        "iot:ListPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPolicyVersions",
        "iot:ListPrincipalPolicies",
        "iot:ListPrincipalThings",
        "iot:ListRoleAliases",
        "iot:ListStreams",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroups",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:ListThingRegistrationTaskReports",
        "iot:ListThingRegistrationTasks",
        "iot:ListThings",
        "iot:ListThingsInThingGroup",
        "iot:ListThingTypes",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:SearchIndex",
        "iot:TestAuthorization",
        "iot:TestInvokeAuthorizer",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuditTask",
        "iot:ListAuditTasks",
        "iot:DescribeScheduledAudit",
        "iot:ListScheduledAudits",
        "iot:ListAuditFindings",
        "iot:DescribeSecurityProfile",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListActiveViolations",
        "iot:ListViolationEvents",
        "iot:ValidateSecurityProfileBehaviors"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoTDataAccess

`AWSIoTDataAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan akses penuh ke tindakan pesanAWS IoT

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTDataAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Oktober 2015, 21:51 UTC
- Waktu yang telah diedit: 23 Juni 2021 21.34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDataAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:Connect",
        "iot:Publish",
        "iot:Subscribe",
        "iot:Receive",
        "iot:GetThingShadow",
        "iot:UpdateThingShadow",
        "iot:DeleteThingShadow",
        "iot:ListNamedShadowsForThing"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

`AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`adalah kebijakanAWS terkelola yang: Menyediakan akses tulis ke grup hal IoT dan akses baca ke Sertifikat IoT untuk eksekusi tindakan mitigasi ADD_THINGS_TO_THING_GROUP

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Agustus 2019, 17:55 UTC
- Waktu yang telah diedit: 07 Agustus 2019 17.55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:ListPrincipalThings",
        "iot:AddThingToThingGroup"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIoTDeviceDefenderAudit

`AWSIoTDeviceDefenderAudit`adalah kebijakanAWS terkelola yang: Menyediakan akses baca untuk IoT dan sumber daya terkait

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTDeviceDefenderAudit` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 18 Juli 2018, 21:17 UTC
- Waktu yang telah diedit: 25 November 2019 23.52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:GetLoggingOptions",
        "iot:GetV2LoggingOptions",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:ListPolicies",
        "iot:GetPolicy",
        "iot:GetEffectivePolicies",
        "iot:ListRoleAliases",
        "iot:DescribeRoleAlias",
        "cognito-identity:GetIdentityPoolRoles",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetails"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

`AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk mengaktifkan pencatatan IoT untuk eksekusi tindakan mitigasi ENABLE_IOT_LOGGING

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Agustus 2019, 17:04 UTC
- Waktu yang telah diedit: 07 Agustus 2019 17.04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

`AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`adalah kebijakanAWS terkelola yang: Menyediakan pesan yang mempublikasikan akses ke topik SNS untuk eksekusi aksi mitigasi PUBLISH_FINDING_TO_SNS

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Agustus 2019, 17:04 UTC
- Waktu yang telah diedit: 07 Agustus 2019 17.04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

`AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`adalah kebijakanAWS terkelola yang: Menyediakan akses tulis ke kebijakan IoT untuk eksekusi tindakan mitigasi REPLACE_DEFAULT_POLICY_VERSION

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Agustus 2019, 17:04 UTC
- Waktu yang telah diedit: 07 Agustus 2019 17.04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicyVersion"
```

```
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIoTDeviceDefenderUpdateCACertMitigationAction

`AWSIoTDeviceDefenderUpdateCACertMitigationAction`adalah kebijakanAWS terkelola yang: Menyediakan akses tulis ke sertifikat IoT CA untuk eksekusi tindakan mitigasi UPDATE_CA_CERTIFICATE

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTDeviceDefenderUpdateCACertMitigationAction` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Agustus 2019, 17:05 UTC
- Waktu yang telah diedit: 07 Agustus 2019 17.05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:UpdateCACertificate"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

`AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`adalah kebijakanAWS terkelola yang: Menyediakan akses tulis ke sertifikat IoT untuk eksekusi tindakan mitigasi UPDATE_DEVICE_CERTIFICATE

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 Agustus 2019, 17:06 UTC
- Waktu yang telah diedit: 07 Agustus 2019 17.06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:UpdateCertificate"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIoTDeviceTesterForFreeRTOSFullAccess

`AWSIoTDeviceTesterForFreeRTOSFullAccess`adalah sebuahAWSkebijakan terkelolaitu: MemungkinkanAWSIoT Device Tester untuk menjalankan rangkaian kualifikasi FreeRTOS dengan mengizinkan akses ke layanan termasuk IoT, S3, dan IAM

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTDeviceTesterForFreeRTOSFullAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Tipe:AWSkebijakan terkelola
- Waktu pembuatan: 12 Februari 2020, 20:33 UTC
- Waktu yang diedit:10 Agustus 2023, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

Versi kebijakan

Versi kebijakan: v7(default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber dayaAWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : "arn:aws:iam::*:role/idt-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "iot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteThing",
        "iot:AttachThingPrincipal",
        "iot:DeleteCertificate",
        "iot:GetRegistrationCode",
        "iot:CreatePolicy",
        "iot:UpdateCACertificate",
        "s3:ListBucket",
        "iot:DescribeEndpoint",
        "iot:CreateOTAUpdate",
        "iot:CreateStream",
        "signer:ListSigningJobs",
        "acm:ListCertificates",
        "iot:CreateKeysAndCertificate",
        "iot:UpdateCertificate",
        "iot:CreateCertificateFromCsr",
        "iot:DetachThingPrincipal",
        "iot:RegisterCACertificate",
        "iot:CreateThing",
        "iam:ListRoles",
        "iot:RegisterCertificate",
        "iot:DeleteCACertificate",
        "signer:PutSigningProfile",
        "s3:ListAllMyBuckets",
        "signer:ListSigningPlatforms",
        "iot-device-tester:SendMetrics",
        "iot-device-tester:SupportedVersion",
        "iot-device-tester:LatestIdt",
        "iot-device-tester:CheckVersion",
        "iot-device-tester:DownloadTestSuite"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "signer:StartSigningJob",
        "acm:GetCertificate",
        "signer:DescribeSigningJob",
        "s3:CreateBucket",
        "execute-api:Invoke",
        "s3:DeleteBucket",
        "s3:PutBucketVersioning",
        "signer:CancelSigningProfile"
      ],
      "Resource" : [
        "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
        "arn:aws:signer:*:*:/signing-profiles/*",
        "arn:aws:signer:*:*:/signing-jobs/*",
        "arn:aws:iam::*:role/idt-*",
        "arn:aws:acm:*:*:certificate/*",
        "arn:aws:s3:::idt-*",
        "arn:aws:s3:::afr-ota*"
      ]
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteStream",
        "iot:DeleteCertificate",
        "iot:AttachPolicy",
        "iot:DetachPolicy",
        "iot:DeletePolicy",
        "s3:ListBucketVersions",
        "iot:UpdateCertificate",
        "iot:GetOTAUpdate",
        "iot:DeleteOTAUpdate",
        "iot:DescribeJobExecution"
      ],
      "Resource" : [
        "arn:aws:s3:::afr-ota*",
        "arn:aws:iot:*:*:thinggroup/idt*",
        "arn:aws:iam::*:role/idt-*"
      ]
    },
```

```
    {
      "Sid" : "VisualEditor4",
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteCertificate",
        "iot:AttachPolicy",
        "iot:DetachPolicy",
        "s3:DeleteObjectVersion",
        "iot:DeleteOTAUpdate",
        "s3:PutObject",
        "s3:GetObject",
        "iot:DeleteStream",
        "iot:DeletePolicy",
        "s3:DeleteObject",
        "iot:UpdateCertificate",
        "iot:GetOTAUpdate",
        "s3:GetObjectVersion",
        "iot:DescribeJobExecution"
      ],
      "Resource" : [
        "arn:aws:s3:::afr-ota*/*",
        "arn:aws:s3:::idt-*/*",
        "arn:aws:iot:*:*:policy/idt*",
        "arn:aws:iam::*:role/idt-*",
        "arn:aws:iot:*:*:otaupdate/idt*",
        "arn:aws:iot:*:*:thing/idt*",
        "arn:aws:iot:*:*:cert/*",
        "arn:aws:iot:*:*:job/*",
        "arn:aws:iot:*:*:stream/*"
      ]
    },
    {
      "Sid" : "VisualEditor5",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::afr-ota*/*",
        "arn:aws:s3:::idt-*/*"
      ]
    },
    {
```

```
      "Sid" : "VisualEditor6",
      "Effect" : "Allow",
      "Action" : [
        "iot:CancelJobExecution"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:job/*",
        "arn:aws:iot:*:*:thing/idt*"
      ]
    },
    {
      "Sid" : "VisualEditor7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor9",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "VisualEditor11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Owner" : "IoTDeviceTester"
        }
      }
    },
```

```
    {
      "Sid" : "VisualEditor12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ssm:DescribeParameters",
        "ssm:GetParameters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "Owner"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateSecurityGroup"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai denganAWSkebijakan terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTDeviceTesterForGreengrassFullAccess

`AWSIoTDeviceTesterForGreengrassFullAccess`adalah kebijakanAWS terkelola yang: MemungkinkanAWS IoT Device Tester untuk menjalankan rangkaian kualifikasiAWS Greengrass dengan memungkinkan akses ke layanan terkait termasuk Lambda, IoT, API Gateway, IAM

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTDeviceTesterForGreengrassFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 20 Februari 2020, 21:21 UTC
- Waktu yang telah diedit: 25 Juni 2020, 17.01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : "arn:aws:iam::*:role/idt-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com",
            "lambda.amazonaws.com",
            "greengrass.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "iot:DeleteCertificate",
        "lambda:DeleteFunction",
        "execute-api:Invoke",
        "iot:UpdateCertificate"
      ],
      "Resource" : [
        "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
        "arn:aws:lambda:*:*:function:idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor4",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPolicy",
```

```
        "iot:DetachPolicy",
        "iot:DeletePolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor5",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateJob",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DeleteJob"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/idt-*",
        "arn:aws:iot:*:*:job/*"
      ]
    },
    {
      "Sid" : "VisualEditor6",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint",
        "greengrass:*",
        "iam:ListAttachedRolePolicies",
        "iot:CreatePolicy",
        "iot:GetThingShadow",
        "iot:CreateKeysAndCertificate",
        "iot:ListThings",
        "iot:UpdateThingShadow",
        "iot:CreateCertificateFromCsr",
        "iot-device-tester:SendMetrics",
        "iot-device-tester:SupportedVersion",
        "iot-device-tester:LatestIdt",
        "iot-device-tester:CheckVersion",
        "iot-device-tester:DownloadTestSuite"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "VisualEditor7",
      "Effect" : "Allow",
      "Action" : [
        "iot:DetachThingPrincipal",
        "iot:AttachThingPrincipal"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:DeleteObjectVersion",
        "s3:ListBucketVersions",
        "s3:CreateBucket",
        "s3:DeleteObject",
        "s3:DeleteBucket"
      ],
      "Resource" : "arn:aws:s3:::idt*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoTEventsFullAccess

`AWSIoTEventsFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke IoT Events.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTEventsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 10 Januari 2019, 22:51 UTC
- Waktu yang telah diedit: 10 Januari 2019 02.51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotevents:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoTEventsReadOnlyAccess

`AWSIoTEventsReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke IoT Events.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTEventsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 10 Januari 2019, 22:50 UTC
- Waktu yang telah diedit: 23 September 2019 07.22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotevents:Describe*",
        "iotevents:List*"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoTFleetHubFederationAccess

`AWSIoTFleetHubFederationAccess`adalah kebijakanAWS terkelola yang: Akses Federasi untuk aplikasi IoT Fleet Hub

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTFleetHubFederationAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 15 Desember 2020, 08:08 UTC
- Waktu yang telah diedit: 04 April 2022, 18.03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTFleetHubFederationAccess`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeIndex",
        "iot:DescribeThingGroup",
        "iot:GetBucketsAggregation",
        "iot:GetCardinality",
        "iot:GetIndexingConfiguration",
        "iot:GetPercentiles",
        "iot:GetStatistics",
        "iot:SearchIndex",
        "iot:CreateFleetMetric",
        "iot:ListFleetMetrics",
        "iot:DeleteFleetMetric",
        "iot:DescribeFleetMetric",
        "iot:UpdateFleetMetric",
        "iot:DescribeCustomMetric",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListMetricValues",
        "iot:ListThingGroups",
        "iot:ListThingsInThingGroup",
        "iot:ListJobTemplates",
        "iot:DescribeJobTemplate",
        "iot:ListJobs",
        "iot:CreateJob",
        "iot:CancelJob",
        "iot:DescribeJob",
        "iot:ListJobExecutionsForJob",
        "iot:ListJobExecutionsForThing",
        "iot:DescribeJobExecution",
        "iot:ListSecurityProfiles",
        "iot:DescribeSecurityProfile",
        "iot:ListActiveViolations",
        "iot:GetThingShadow",
        "iot:ListNamedShadowsForThing",
        "iot:CancelJobExecution",
        "iot:DescribeEndpoint",
```

```
        "iotfleethub:DescribeApplication",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListSubscriptionsByTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:iotfleethub*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:iotfleethub*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoTFleetwiseServiceRolePolicy

`AWSIoTFleetwiseServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memberikan izin kepadaAWS Sumber Daya dan MetaData yang digunakan atau dikelola oleh AWSIoTFleetwise untuk fitur tambahan

Menggunakan kebijakan ini JSON JSON JSON

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Kebijakan tidak dapat melampirkan kebijakan ini tidak dapat melampirkan kebijakan ini tidak dapat dilampirkan kebijakan ini tidak dapat melampirkan kebijakan ini tidak dapat dilampirkan

Rincian kebijakan JJSON JSON

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 September 2022, 23:27 UTC
- Waktu yang telah diedit: 21 September 2022, 23.27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTFleetwiseServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Kebijakan ini adalah versi yang mengizinkan untuk versi yang mengizinkan untuk versi yang mengizinkan untuk versi yang mengizinkan untuk versi yang mengizinkan untuk versi yang mengizinkan untuk versi yang mengizinkan untuk versi Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON SON SON SON SON SON SON SON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/IoTFleetWise"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoTFullAccess

`AWSIoTFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan akses penuh ke konfigurasiAWS IoT dan tindakan pesan

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 Oktober 2015, 15:19 UTC
- Waktu yang telah diedit: 19 Mei 2022, 21.39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:*",
        "iotjobsdata:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIoTLogging

`AWSIoTLogging`adalah kebijakanAWS terkelola yang: Memungkinkan pembuatan grup Amazon CloudWatch Log dan streaming log ke grup

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTLogging` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 08 Oktober 2015, 15:17 UTC
- Waktu yang telah diedit: 08 Oktober 2015 15.17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTLogging`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy",
        "logs:GetLogEvents",
        "logs:DeleteLogStream"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoTOTAUpdate

`AWSIoTOTAUpdate`adalah kebijakanAWS terkelola yang: Memungkinkan akses untuk membuat JobAWS IoT dan menjelaskan pekerjaan penandatanganAWS kode

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTOTAUpdate` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 Desember 2017, 20:36 UTC
- Waktu yang telah diedit: 20 Desember 2017 20.36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan kebijakan kebijakan kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "iot:CreateJob",
      "signer:DescribeSigningJob"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIotRoboRunnerFullAccess

`AWSIotRoboRunnerFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin yang memungkinkan akses penuh keAWS Iot RoboRunner.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIotRoboRunnerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 November 2021, 03:54 UTC
- Waktu yang telah diedit: 23 Pebruari 2023, 18.34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iotroborunner:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/iotroborunner.amazonaws.com/
AWSServiceRoleForIoTRoboRunner",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "iotroborunner.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIotRoboRunnerReadOnly

`AWSIotRoboRunnerReadOnly`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin yang mengizinkan akses hanya baca keAWS IoT RoboRunner.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIotRoboRunnerReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 November 2021, 03:43 UTC
- Waktu yang telah diedit: 16 November 2022, 20.51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerReadOnly`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotroborunner:GetSite",
        "iotroborunner:GetWorker",
        "iotroborunner:ListWorkerFleets",
        "iotroborunner:ListSites",
        "iotroborunner:ListWorkers",
        "iotroborunner:GetDestination",
        "iotroborunner:GetWorkerFleet",
        "iotroborunner:ListDestinations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIotRoboRunnerServiceRolePolicy

`AWSIotRoboRunnerServiceRolePolicy`adalah kebijakanAWS terkelola yang: MemungkinkanAWS IoT RoboRunner untuk mengelolaAWS Sumber Daya terkait atas nama pelanggan.

Menggunakan kebijakan ini menggunakan kebijakan ini menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini tidak dapat dilampirkan pada pengguna, peran, atau peran peran peran peran peran Anda.

Rincian kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Februari 2023, 16:56 UTC
- Waktu yang telah diedit: 21 Pebruari 2023, 16.56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIotRoboRunnerServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan kebijakan kebijakan kebijakan default kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan standar kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan default kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan default kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan Ketika pengguna

atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan JSON JSON JSON JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/Usage"
        ]
      }
    }
  }
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoTRuleActions

`AWSIoTRuleActions`adalah kebijakanAWS terkelola yang: Memungkinkan akses ke semuaAWS layanan yang didukung dalam Tindakan AturanAWS IoT

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTRuleActions` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 08 Oktober 2015, 15:14 UTC
- Waktu yang telah diedit: 16 Januari 2018 07.28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "dynamodb:PutItem",
      "kinesis:PutRecord",
      "iot:Publish",
      "s3:PutObject",
      "sns:Publish",
      "sqs:SendMessage*",
      "cloudwatch:SetAlarmState",
      "cloudwatch:PutMetricData",
      "es:ESHttpPut",
      "firehose:PutRecord"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIoTSiteWiseConsoleFullAccess

`AWSIoTSiteWiseConsoleFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh untuk mengelolaAWS IoT SiteWise menggunakanAWS Management Console. Perhatikan kebijakan ini juga memberikan akses untuk membuat dan mencantumkan penyimpanan data yang digunakan denganAWS IoT SiteWise (misalnyaAWS IoT Analytics), akses ke daftar dan melihat sumber dayaAWS IoT Greengrass, membuat daftar dan memodifikasiAWS rahasia Secrets Manager, mengambil bayanganAWS IoT, mencantumkan sumber daya dengan tag tertentu, dan membuat dan menggunakan peran terkait layanan untukAWS IoT SiteWise.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTSiteWiseConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 31 Mei 2019
- Waktu yang telah diedit: 31 Mei 2019 09.37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Action" : "iotsitewise:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iotanalytics:List*",
        "iotanalytics:Describe*",
        "iotanalytics:Create*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iot:DescribeEndpoint",
        "iot:GetThingShadow"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:ListGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "secretsmanager:ListSecrets",
        "secretsmanager:CreateSecret"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "secretsmanager:UpdateSecret"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
    },
    {
      "Action" : [
        "tag:GetResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "iotsitewise.amazonaws.com"
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "iotsitewise.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIoTSiteWiseFullAccess

`AWSIoTSiteWiseFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke IoT SiteWise.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTSiteWiseFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 04 Desember 2018, 20:53 UTC
- Waktu yang telah diedit: 04 Desember 2018 20.53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:*"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIoTSiteWiseMonitorPortalAccess

`AWSIoTSiteWiseMonitorPortalAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin untuk mengakses SiteWise aset dan data asetAWS IoT, membuat sumber daya SiteWise MonitorAWS IoT, dan mencantumkan penggunaAWS SSO.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTSiteWiseMonitorPortalAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 19 Mei 2020, 20:01 UTC
- Waktu yang telah diedit: 19 Mei 2020, 20.01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen JSON kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:CreateProject",
        "iotsitewise:DescribeProject",
        "iotsitewise:UpdateProject",
        "iotsitewise:DeleteProject",
        "iotsitewise:ListProjects",
        "iotsitewise:BatchAssociateProjectAssets",
        "iotsitewise:BatchDisassociateProjectAssets",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:CreateDashboard",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:UpdateDashboard",
        "iotsitewise:DeleteDashboard",
        "iotsitewise:ListDashboards",
        "iotsitewise:CreateAccessPolicy",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:UpdateAccessPolicy",
        "iotsitewise:DeleteAccessPolicy",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:DescribeAsset",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetAssetPropertyAggregates",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIoTSiteWiseMonitorServiceRolePolicy

`AWSIoTSiteWiseMonitorServiceRolePolicy`adalah kebijakanAWS terkelola yang: Peran ini memberikan izin SiteWise monitorAWS IoT untuk mengakses SiteWise aset & properti asetAWS IoT Anda, dan membuatAWS proyek, dasbor & kebijakan akses IoT Sitewise melalui SiteWise portalAWS IoT.

kebijakan ini kebijakan kebijakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

detail kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 November 2019, 00:59 UTC
- Waktu yang telah diedit: 13 Desember 2019, 22.19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan kebijakan standar kebijakan kebijakan standar kebijakan kebijakan kebijakan kebijakan kebijakan standar kebijakan kebijakan standar kebijakan kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:CreateProject",
        "iotsitewise:DescribeProject",
        "iotsitewise:UpdateProject",
        "iotsitewise:DeleteProject",
        "iotsitewise:ListProjects",
        "iotsitewise:BatchAssociateProjectAssets",
        "iotsitewise:BatchDisassociateProjectAssets",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:CreateDashboard",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:UpdateDashboard",
        "iotsitewise:DeleteDashboard",
        "iotsitewise:ListDashboards",
        "iotsitewise:CreateAccessPolicy",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:UpdateAccessPolicy",
        "iotsitewise:DeleteAccessPolicy",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:DescribeAsset",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetAssetPropertyAggregates",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIoTSiteWiseReadOnlyAccess

`AWSIoTSiteWiseReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke IoT SiteWise.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTSiteWiseReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 04 Desember 2018, 20:55 UTC
- Waktu yang telah diedit: 16 September 2022, 19.05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:Describe*",
        "iotsitewise:List*",
        "iotsitewise:Get*",
        "iotsitewise:BatchGet*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIoTThingsRegistration

`AWSIoTThingsRegistration`adalah kebijakanAWS terkelola yang: Kebijakan ini memungkinkan pengguna untuk mendaftarkan barang secara massal menggunakanAWS IoT StartThingRegistrationTask API

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTThingsRegistration` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Desember 2017, 20:21 UTC
- Waktu yang telah diedit: 05 Oktober 2020, 19.20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:AddThingToThingGroup",
        "iot:AttachPolicy",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CreateCertificateFromCsr",
        "iot:CreatePolicy",
        "iot:CreateThing",
        "iot:DescribeCertificate",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:DetachPolicy",
        "iot:DetachThingPrincipal",
        "iot:GetPolicy",
        "iot:ListAttachedPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPrincipalPolicies",
        "iot:ListPrincipalThings",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:RegisterCertificate",
        "iot:RegisterThing",
        "iot:RemoveThingFromThingGroup",
        "iot:UpdateCertificate",
        "iot:UpdateThing",
        "iot:UpdateThingGroupsForThing",
```

```
        "iot:AddThingToBillingGroup",
        "iot:DescribeBillingGroup",
        "iot:RemoveThingFromBillingGroup"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoTTwinMakerServiceRolePolicy

`AWSIoTTwinMakerServiceRolePolicy`adalah kebijakan AWS terkelola yang: Memungkinkan AWS IoT TwinMaker memanggil AWS layanan lain dan menyinkronkan sumber daya mereka atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 November 2023, 18:59 UTC
- Waktu telah diedit: 13 November 2023, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTTwinMakerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SiteWiseAssetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:DescribeAsset"
      ],
      "Resource" : [
        "arn:aws:iotsitewise:*:*:asset/*"
      ]
    },
    {
      "Sid" : "SiteWiseAssetModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:DescribeAssetModel"
      ],
      "Resource" : [
        "arn:aws:iotsitewise:*:*:asset-model/*"
      ]
    },
    {
      "Sid" : "SiteWiseAssetModelAndAssetListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssetModels"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "TwinMakerAccess",
      "Effect" : "Allow",
      "Action" : [
        "iottwinmaker:GetEntity",
        "iottwinmaker:CreateEntity",
        "iottwinmaker:UpdateEntity",
        "iottwinmaker:DeleteEntity",
        "iottwinmaker:ListEntities",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:CreateComponentType",
        "iottwinmaker:UpdateComponentType",
        "iottwinmaker:DeleteComponentType",
        "iottwinmaker:ListComponentTypes"
      ],
      "Resource" : [
        "arn:aws:iottwinmaker:*:*:workspace/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iottwinmaker:linkedServices" : [
            "IOTSITEWISE"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIoTWirelessDataAccess

`AWSIoTWirelessDataAccess`adalah kebijakanAWS terkelola yang: Memungkinkan akses data identitas terkait ke perangkatAWS IoT Wireless.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTWirelessDataAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 15 Desember 2020, 15:31 UTC
- Waktu yang telah diedit: 15 Desember 2020, 15.31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotwireless:SendDataToWirelessDevice"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIoTWirelessFullAccess

`AWSIoTWirelessFullAccess`adalah kebijakanAWS terkelola yang: Memungkinkan akses penuh identitas terkait ke semua operasiAWS IoT Wireless.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTWirelessFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 15 Desember 2020, 15:27 UTC
- Waktu yang telah diedit: 15 Desember 2020, 15.27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotwireless:*"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIoTWirelessFullPublishAccess

`AWSIoTWirelessFullPublishAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh IoT Wireless untuk mempublikasikan ke IoT Rules Engine atas nama Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTWirelessFullPublishAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 15 Desember 2020, 15:29 UTC
- Waktu yang telah diedit: 15 Desember 2020, 15.29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint",
        "iot:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIoTWirelessGatewayCertManager

`AWSIoTWirelessGatewayCertManager`adalah kebijakanAWS terkelola yang: Memungkinkan akses identitas terkait untuk membuat, mencantumkan, dan menjelaskan Sertifikat IoT

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTWirelessGatewayCertManager` ke pengguna, grup, dan peran Anda.

Rincian kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 15 Desember 2020, 15:30 UTC
- Waktu yang telah diedit: 15 Desember 2020 15.30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan kebijakan adalah versi yang menentukan izin untuk kebijakan kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON kebijakan kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan izin identitas IAM M M M M M M M M M M M M M
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIoTWirelessLogging

`AWSIoTWirelessLogging`adalah kebijakanAWS terkelola yang: Memungkinkan identitas terkait untuk membuat grup Amazon CloudWatch Logs dan melakukan streaming log ke grup.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTWirelessLogging` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 15 Desember 2020, 15:32 UTC
- Waktu yang telah diedit: 15 Desember 2020, 15.32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessLogging`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotwireless*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIoTWirelessReadOnlyAccess

`AWSIoTWirelessReadOnlyAccess`adalah kebijakanAWS terkelola yang: Memungkinkan akses hanya baca identitas terkait ke nirkabelAWS IoT.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIoTWirelessReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 15 Desember 2020, 15:28 UTC
- Waktu yang telah diedit: 15 Desember 2020, 15.28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iotwireless:List*",
        "iotwireless:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIPAMServiceRolePolicy

`AWSIPAMServiceRolePolicy`adalah kebijakan AWS terkelola yang: Memungkinkan Manajer Alamat IP VPC mengakses sumber daya VPC dan berintegrasi dengan AWS Organizations atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 November 2021, 19:08 UTC
- Waktu telah diedit: November 08, 2023, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IPAMDiscoveryDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListByoipCidrs",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchMetricsPublishActions",
      "Effect" : "Allow",
```

```
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/IPAM"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSIQContractServiceRolePolicy

`AWSIQContractServiceRolePolicy`adalah kebijakanAWS terkelola yang: Digunakan olehAWS IQ untuk mengeksekusi permintaan pembayaran atas nama pelanggan

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 22 Agustus 2019, 19:28 UTC
- Waktu yang telah diedit: 22 Agustus 2019 08.28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:Subscribe"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSIQFullAccess

`AWSIQFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS IQ

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSIQFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 04 April 2019, 23:13 UTC
- Waktu yang telah diedit: 25 September 2019 20.22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIQFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iq:*",
        "iq-permission:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "permission.iq.amazonaws.com",
            "contract.iq.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSIQPermissionServiceRolePolicy

`AWSIQPermissionServiceRolePolicy`adalah kebijakanAWS terkelola yang: MemungkinkanAWS IQ mengelola peran yang diasumsikan oleh para ahliAWS IQ.

Menggunakan kebijakan kebijakan kebijakan ini kebijakan kebijakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan tidak dapat melampirkan kebijakan tidak dapat melampirkan kebijakan ini tidak dapat dilampirkan kebijakan ini tidak dapat dilampirkan kebijakan ini

detail kebijakan kebijakan kebijakan detail kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 22 Agustus 2019, 19:36 UTC
- Waktu yang telah diedit: 22 Agustus 2019 19.36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi standar versi kebijakan ini adalah versi yang menentukan izin untuk versi kebijakan yang mengizinkan versi kebijakan yang mengizinkan versi kebijakan yang mengizinkan versi kebijakan yang mengizinkan versi kebijakan kebijakan yang mengizinkan versi kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSDenyAll"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

`AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`adalah kebijakan AWS terkelola yang: Mengaktifkan akses ke AWS layanan dan sumber daya yang diperlukan untuk AWS penyimpanan kunci khusus KMS

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 November 2018, 20:10 UTC
- Waktu telah diedit: 10 November 2023, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:Describe*",
```

```
        "ec2:CreateNetworkInterface",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

`AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`adalah kebijakanAWS terkelola yang: MemungkinkanAWS KMS untuk menyinkronkan properti bersama kunci Multi-wilayah.

Menggunakan kebijakan ini terkait kebijakan ini dilampirkan

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini tidak dapat peran Anda.

Rincian kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 16 Juni 2021, 15:37 UTC
- Waktu yang telah diedit: 16 Juni 2021 15.37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan default adalah versi yang menentukan versi default default terkait versi default. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan JSON SON SON SON SON SON SON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:SynchronizeMultiRegionKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSKeyManagementServicePowerUser

`AWSKeyManagementServicePowerUser`adalah kebijakanAWS terkelola yang: Menyediakan akses keAWS Key Management Service (KMS).

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSKeyManagementServicePowerUser` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 07 Maret 2017, 00.55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms:DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
        "kms:List*",
        "kms:TagResource",
        "kms:UntagResource",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSLakeFormationCrossAccountManager

`AWSLakeFormationCrossAccountManager`adalah kebijakan AWS terkelola yang: Menyediakan akses lintas akun ke sumber daya Glue melalui Lake Formation. Juga memberikan akses baca ke layanan lain yang diperlukan seperti organisasi dan manajer akses sumber daya

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLakeFormationCrossAccountManager` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 Agustus 2020, 20:59 UTC
- Waktu telah diedit: November 01, 2023, 00:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceSharePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:PermissionArn" : [
```

```
            "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:PutResourcePolicy",
        "glue:DeleteResourcePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "ram:Get*",
        "ram:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLakeFormationDataAdmin

`AWSLakeFormationDataAdmin`adalah kebijakanAWS terkelola yang: Memberikan akses administratif keAWS Lake Formation dan layanan terkait, sepertiAWS Glue, untuk mengelola danau data

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSLakeFormationDataAdmin` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 Agustus 2019, 17:33 UTC
- Waktu yang telah diedit: 16 Desember 2019 02.41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:CreateDatabase",
```

```
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:GetConnections",
        "glue:SearchTables",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:GetTableVersions",
        "glue:GetPartitions",
        "glue:GetTables",
        "glue:GetWorkflow",
        "glue:ListWorkflows",
        "glue:BatchGetWorkflows",
        "glue:DeleteWorkflow",
        "glue:GetWorkflowRuns",
        "glue:StartWorkflowRun",
        "glue:GetWorkflow",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "iam:ListUsers",
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "lakeformation:PutDataLakeSettings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSLambda_FullAccess

`AWSLambda_FullAccess`adalah kebijakanAWS terkelola yang: Memberikan akses penuh ke layananAWS Lambda, fitur konsolAWS Lambda, danAWS layanan terkait lainnya.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSLambda_FullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 17 November 2020, 21:14 UTC
- Waktu yang telah diedit: 17 November 2020, 21.14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_FullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "lambda:*",
        "logs:DescribeLogGroups",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSLambda_ReadOnlyAccess

`AWSLambda_ReadOnlyAccess`adalahAWSkebijakan terkelolabahwa: Memberikan akses hanya-baca keAWSLayanan Lambda,AWSFitur konsol Lambda, dan terkait lainnyaAWSlayanan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSLambda_ReadOnlyAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 17 November 2020, 21:10 UTC
- Waktu yang diedit:27 Juli 2023, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "lambda:Get*",
        "lambda:List*",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:DescribeQueries",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
        "logs:GetQueryResults"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSLambdaBasicExecutionRole

`AWSLambdaBasicExecutionRole`adalah kebijakanAWS terkelola yang: Menyediakan izin tulis ke CloudWatch Log.

Menggunakan kebijakan

Anda dapat melampirkan`AWSLambdaBasicExecutionRole` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 April 2015, 15:03 UTC
- Waktu yang telah diedit: 09 April 2015 15.03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSLambdaDynamoDBExecutionRole

`AWSLambdaDynamoDBExecutionRole`adalah kebijakanAWS terkelola yang: Menyediakan daftar dan akses baca ke aliran DynamoDB dan menulis izin untuk CloudWatch log.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSLambdaDynamoDBExecutionRole` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 April 2015, 15:09 UTC
- Waktu yang telah diedit: 09 April 2015 15.09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSLambdaENIManagementAccess

`AWSLambdaENIManagementAccess`adalah kebijakanAWS terkelola yang: Menyediakan izin minimum untuk fungsi Lambda untuk mengelola ENI (membuat, menjelaskan, menghapus) yang digunakan oleh Fungsi Lambda berkemampuan VPC.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSLambdaENIManagementAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Desember 2016, 00:37 UTC
- Waktu yang telah diedit: 01 Oktober 2020 20.07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSLambdaExecute

`AWSLambdaExecute`adalah kebijakanAWS terkelola yang: Menyediakan Put, Dapatkan akses ke S3 dan akses penuh ke CloudWatch Log.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSLambdaExecute` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 08.40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaExecute`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSLambdaFullAccess

`AWSLambdaFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini berada di jalur pengusangan. Lihat dokumentasi untuk panduan: https://docs.aws.amazon.com/lambda/latest/dg/access-control-identity-based .html. Menyediakan akses penuh ke Lambda, S3, DynamoDB, CloudWatch Metrics dan Log.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSLambdaFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 27 November 2017 08.22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaFullAccess`

Versi kebijakan

Versi kebijakan:v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudwatch:*",
        "cognito-identity:ListIdentityPools",
        "cognito-sync:GetCognitoEvents",
        "cognito-sync:SetCognitoEvents",
        "dynamodb:*",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
```

```
        "events:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:PassRole",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy",
        "iot:CreateThing",
        "iot:CreateTopicRule",
        "iot:DescribeEndpoint",
        "iot:GetTopicRule",
        "iot:ListPolicies",
        "iot:ListThings",
        "iot:ListTopicRules",
        "iot:ReplaceTopicRule",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kms:ListAliases",
        "lambda:*",
        "logs:*",
        "s3:*",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Publish",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sqs:ListQueues",
        "sqs:SendMessage",
        "tag:GetResources",
        "xray:PutTelemetryRecords",
        "xray:PutTraceSegments"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSLambdaInvocation-DynamoDB

`AWSLambdaInvocation-DynamoDB`adalah kebijakanAWS terkelola yang: Menyediakan akses baca ke DynamoDB Streams.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSLambdaInvocation-DynamoDB` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 08.40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSLambdaKinesisExecutionRole

`AWSLambdaKinesisExecutionRole`adalah kebijakanAWS terkelola yang: Menyediakan daftar dan akses baca ke aliran Kinesis dan izin menulis ke CloudWatch log.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSLambdaKinesisExecutionRole` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 April 2015, 15:14 UTC
- Waktu yang telah diedit: 19 November 2018 20.09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetRecords",
        "kinesis:GetShardIterator",
        "kinesis:ListShards",
        "kinesis:ListStreams",
        "kinesis:SubscribeToShard",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSLambdaMSKExecutionRole

`AWSLambdaMSKExecutionRole`adalah kebijakanAWS terkelola yang: Menyediakan izin yang diperlukan untuk mengakses Cluster MSK dalam VPC, mengelola ENI (membuat, menjelaskan, menghapus) di VPC dan menulis izin untuk CloudWatch Log.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSLambdaMSKExecutionRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 Agustus 2020, 17:35 UTC
- Waktu yang telah diedit: 02 Agustus 2022, 20.08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:GetBootstrapBrokers",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSLambdaReplicator

`AWSLambdaReplicator`adalah kebijakanAWS terkelola yang: Memberikan izin yang diperlukan kepada Lambda Replicator untuk mereplikasi fungsi di seluruh wilayah

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 Mei 2017, 17:53 UTC
- Waktu yang telah diedit: 08 Desember 2017, 00:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LambdaCreateDeletePermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:DisableReplication"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "IamPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
```

```
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFrontListDistributions",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionsByLambdaFunction"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSLambdaRole

`AWSLambdaRole`adalah kebijakanAWS terkelola yang: Kebijakan default untuk peran layananAWS Lambda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSLambdaRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 18.41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaRole`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSLambdaSQSQueueExecutionRole

`AWSLambdaSQSQueueExecutionRole`adalah kebijakanAWS terkelola yang: Menyediakan pesan terima, menghapus pesan, dan akses atribut baca ke antrian SQS, dan menulis izin untuk CloudWatch log.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSLambdaSQSQueueExecutionRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Juni 2018, 21:50 UTC
- Waktu yang telah diedit: 14 Juni 2018 09.50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSLambdaVPCAccessExecutionRole

`AWSLambdaVPCAccessExecutionRole`adalah kebijakan AWS terkelola yang: Memberikan izin minimum untuk fungsi Lambda untuk dijalankan saat mengakses sumber daya dalam VPC - buat, jelaskan, hapus antarmuka jaringan, dan tulis izin ke Log. CloudWatch

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSLambdaVPCAccessExecutionRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 Februari 2016, 23:15 UTC
- Waktu telah diedit: 05 Januari 2024, 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLambdaVPCAccessExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSLicenseManagerConsumptionPolicy

`AWSLicenseManagerConsumptionPolicy`adalah kebijakanAWS terkelola yang: Menyediakan izin untuk mengizinkan akses ke tindakan APIAWS License Manager yang diperlukan untuk dikonsumsi pada lisensi yang memiliki hak pengguna.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSLicenseManagerConsumptionPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 Agustus 2021, 23:18 UTC
- Waktu yang telah diedit: 11 Agustus 2021 02.08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan dan dan dan izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

`AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Layanan Langganan LinuxAWS License Manager untuk mengelola sumber daya atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 Desember 2022, 18:54 UTC
- Waktu yang telah diedit: 20 Desember 2022, 18.54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSLicenseManagerMasterAccountRolePolicy

`AWSLicenseManagerMasterAccountRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan peran akun master layananAWS License Manager

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, grup, peran baru.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 November 2018, 19:03 UTC
- Waktu yang telah diedit: 31 Mei 2022, 20.50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "S3ObjectPermissions1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:AbortMultipartUpload",
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "S3ObjectPermissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*/resource_sync/*"
      ]
    },
    {
      "Sid" : "AthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "GluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTable",
        "glue:GetPartition",
        "glue:GetPartitions"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RAMPermissions1",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareAssociations",
        "ram:TagResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RAMPermissions2",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Service" : "LicenseManager"
        }
      }
    },
```

```
    {
      "Sid" : "RAMPermissions3",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Service" : "LicenseManager"
        }
      }
    },
    {
      "Sid" : "IAMGetRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMPassRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/LicenseManagerServiceResourceDataSyncRole*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "cloudformation.amazonaws.com",
            "glue.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "CloudformationPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/
LicenseManagerCrossAccountCloudDiscoveryStack/*"
      ]
    },
    {
      "Sid" : "GlueUpdatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:UpdateJob",
        "glue:UpdateCrawler"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:crawler/LicenseManagerResourceSynDataCrawler",
        "arn:aws:glue:*:*:job/LicenseManagerResourceSynDataProcessJob",
        "arn:aws:glue:*:*:table/license_manager_resource_inventory_db/*",
        "arn:aws:glue:*:*:table/license_manager_resource_sync/*",
        "arn:aws:glue:*:*:database/license_manager_resource_inventory_db",
        "arn:aws:glue:*:*:database/license_manager_resource_sync"
      ]
    },
    {
      "Sid" : "RGPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:PutGroupPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSLicenseManagerMemberAccountRolePolicy

`AWSLicenseManagerMemberAccountRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan peran akun anggota layananAWS License Manager

Kebijakan ini menggunakan kebijakan ini ini kebijakan ini ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Kebijakan ini tidak dapat melampirkan kebijakan ini untuk kebijakan ini tidak dapat dilampirkan kebijakan ini tidak dapat dilampirkan kebijakan ini ke pengguna Anda.

Rincian kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 November 2018, 19:04 UTC
- Waktu yang telah diedit: 15 November 2019 08.09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan JSON JSON kebijakan kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LicenseManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource",
        "license-manager:GetLicenseConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListInventoryEntries",
        "ssm:GetInventory",
        "ssm:CreateAssociation",
        "ssm:CreateResourceDataSync",
        "ssm:DeleteResourceDataSync",
        "ssm:ListResourceDataSync",
        "ssm:ListAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RAMPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSLicenseManagerServiceRolePolicy

`AWSLicenseManagerServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan peran default layananAWS License Manager

Menggunakan kebijakan ini tidak dapat dilampirkan.

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau grup, atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau atau

Rincian kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 November 2018, 19:02 UTC
- Waktu yang telah diedit: 30 Juli 2021 01.43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v7 (default)

Versi default kebijakan default kebijakan ini adalah versi yang menentukan izin untuk kebijakan terkait kebijakan ini. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan JSON JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/license-
management.marketplace.amazonaws.com/AWSServiceRoleForMarketplaceLicenseManagement"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "license-management.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPermissionsForCreatingMemberSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/license-manager.member-
account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "license-manager.member-account.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "S3BucketPermissions1",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "S3BucketPermissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3ObjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "SNSAccountPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "SNSTopicPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeHosts"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListInventoryEntries",
        "ssm:GetInventory",
        "ssm:CreateAssociation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "LicenseManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "license-manager:GetServiceSettings",
        "license-manager:GetLicense*",
        "license-manager:UpdateLicenseSpecificationsForResource",
        "license-manager:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

`AWSLicenseManagerUserSubscriptionsServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Layanan Langganan PenggunaAWS License Manager untuk mengelola sumber daya atas nama Anda.

Menggunakan kebijakan

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, atau peran baru.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 Juli 2022, 01:17 UTC
- Waktu yang telah diedit: 21 November 2022, 19.51 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v3 (default)

Kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetInventory",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVpcPeeringConnections"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2WritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:productCode" : [
            "bz0vcy31ooqlzk5tsash4r1ik",
            "d44g89hc0gp9jdzm99rznthpw",
            "77yzkpa7kvee1y1tt7wnsdwoc"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "SSMDocumentExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunPowerShellScript"
      ]
    },
    {
      "Sid" : "SSMInstanceExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AWSLicenseManager" : "UserSubscriptions"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSM2ServicePolicy

`AWSM2ServicePolicy`adalah kebijakanAWS terkelola yang: MemungkinkanAWS M2 mengelolaAWS sumber daya atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna,

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 Juni 2022, 20:26 UTC
- Waktu yang telah diedit: 07 Juni 2022, 20.26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan ini adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/M2"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSManagedServices_ContactsServiceRolePolicy

`AWSManagedServices_ContactsServiceRolePolicy`adalah kebijakanAWS terkelola yang: MemungkinkanAWS Managed Services untuk membaca nilai tag padaAWS sumber daya

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran baru.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 Maret 2023, 17:07 UTC
- Waktu yang telah diedit: 23 Maret 2023, 17.07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan ini adalah versi yang menentukan izin untuk kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoleTags",
        "iam:ListUserTags",
        "tag:GetResources",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetBucketTagging",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:authType" : "REST-HEADER",
          "s3:signatureversion" : "AWS4-HMAC-SHA256"
        },
        "NumericGreaterThanEquals" : {
          "s3:TlsVersion" : "1.2"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

`AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`adalah kebijakanAWS terkelola yang:AWS Managed Services - kebijakan untuk mengelola infrastruktur kontrol detektif

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat ampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

detail kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 Desember 2022, 23:11 UTC
- Waktu yang telah diedit: 19 Desember 2022, 23.11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateTermination*",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackResources",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/ams-detective-controls-config-recorder",
        "arn:aws:cloudformation:*:*:stack/ams-detective-controls-config-rules-cdk",
        "arn:aws:cloudformation:*:*:stack/ams-detective-controls-infrastructure-cdk"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeAggregationAuthorizations",
        "config:PutAggregationAuthorization",
        "config:TagResource",
        "config:PutConfigRule"
      ],
      "Resource" : [
        "arn:aws:config:*:*:aggregation-authorization/540708452589/*",
        "arn:aws:config:*:*::config-rule/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy",
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetBucketAcl",
```

```
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketLogging",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::ams-config-record-bucket-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSManagedServices_EventsServiceRolePolicy

`AWSManagedServices_EventsServiceRolePolicy`adalah kebijakanAWS terkelola yang: KebijakanAWS Managed Services untuk mengaktifkan fitur prosesor peristiwa AMS.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, grup, atau peran.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 Februari 2023, 18:41 UTC
- Waktu yang telah diedit: 07 Pebruari 2023, 18.41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "events.managedservices.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSManagedServicesDeploymentToolkitPolicy

`AWSManagedServicesDeploymentToolkitPolicy`adalah kebijakanAWS terkelola yang: MemungkinkanAWS Managed Services untuk mengelola toolkit penyebaran atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 09 Juni 2022, 18:33 UTC
- Waktu yang telah diedit: 10 Mei 2023, 17.48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
```

```
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObject",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersion",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketVersioning",
        "s3:GetLifecycleConfiguration",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectAttributes",
        "s3:GetObjectLegalHold",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionAttributes",
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionTorrent",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutBucketAcl",
        "s3:PutBucketLogging",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::ams-cdktoolkit*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeChangeSet",
```

```
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:GetTemplateSummary",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:UpdateTerminationProtection"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:DeleteLifecyclePolicy",
        "ecr:DeleteRepository",
        "ecr:DeleteRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:ListTagsForResource",
        "ecr:PutImageTagMutability",
        "ecr:PutLifecyclePolicy",
        "ecr:SetRepositoryPolicy",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/ams-cdktoolkit*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSMarketplaceAmiIngestion

`AWSMarketplaceAmiIngestion`adalah kebijakanAWS terkelola yang: MemungkinkanAWS Marketplace untuk menyalin Amazon Machine Images (AMI) Anda untuk mendaftarkannyaAWS Marketplace

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMarketplaceAmiIngestion` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 25 September 2020, 20:55 UTC
- Waktu yang telah diedit: 25 September 2020 20.55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:ec2:us-east-1::snapshot/snap-*"
    },
    {
      "Action" : [
```

```
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshotAttribute",
        "ec2:ModifyImageAttribute"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMarketplaceDeploymentServiceRolePolicy

`AWSMarketplaceDeploymentServiceRolePolicy`adalah kebijakan AWS terkelola yang: Memungkinkan AWS Marketplace untuk membuat dan mengelola parameter penyebaran penjual untuk produk yang Anda berlangganan. AWS Marketplace

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 15 November 2023, 23:34 UTC
- Waktu telah diedit: 15 November 2023, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageMarketplaceDeploymentSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:RemoveRegionsFromReplication"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:marketplace-deployment*!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "TagMarketplaceDeploymentSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:marketplace-deployment!*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/expirationDate" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "expirationDate"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceFullAccess

`AWSMarketplaceFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan kemampuan untuk berlangganan dan berhenti berlangganAWS Marketplace perangkat lunak, memungkinkan pengguna untuk mengelola instans perangkat lunak Marketplace dari halaman Marketplace 'Perangkat Lunak', dan menyediakan akses administratif ke EC2.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMarketplaceFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Februari 2015, 17:21 UTC
- Waktu yang telah diedit: 04 Maret 2022, 17.04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceFullAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:CreateImage",
        "ec2:DescribeInstanceStatus",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:DescribeDocument",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:CreateTopic",
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:ListRoles",
        "iam:ListInstanceProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*image-build*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish",
        "sns:setTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:*image-build*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
        "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
        "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
        "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
        "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
        "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
        "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
        "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
            "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
            "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
            "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
            "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
            "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
            "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
            "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMarketplaceGetEntitlements

`AWSMarketplaceGetEntitlements`adalah kebijakanAWS terkelola yang: Menyediakan akses bacaAWS Marketplace ke Hak

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMarketplaceGetEntitlements` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Maret 2017, 19:37 UTC
- Waktu yang telah diedit: 27 Maret 2017 07.37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:GetEntitlements"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSMarketplaceImageBuildFullAccess

`AWSMarketplaceImageBuildFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Fitur Pembuatan GambarAWS Marketplace Pribadi. Selain membuat citra privat, juga menyediakan izin untuk menambahkan tanda ke citra, meluncurkan dan mengakhiri instans ec2.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMarketplaceImageBuildFullAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 31 Juli 2018, 23:29 UTC
- Waktu yang telah diedit: 04 Maret 2022, 17.05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListBuilds",
        "aws-marketplace:StartBuild",
        "aws-marketplace:DescribeBuilds"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/marketplace-image-build:build-id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*Automation*",
        "arn:aws:iam::*:role/*Instance*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:DescribeDocument",
        "ec2:DeregisterImage",
        "ec2:CopyImage",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DeleteSnapshot",
        "ec2:CreateImage",
        "ec2:RunInstances",
        "ec2:DescribeInstanceStatus",
        "sns:GetTopicAttributes",
        "iam:GetRole",
```

```
        "iam:GetInstanceProfile"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*image-build*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*image-build*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
        "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
        "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
        "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
        "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
```

```
        "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
        "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
        "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
            "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
            "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
            "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
            "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
            "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
            "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
            "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/marketplace-image-build:build-id" : "*"
        },
        "StringNotEquals" : {
```

```
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM IAM IAM IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMarketplaceLicenseManagementServiceRolePolicy

`AWSMarketplaceLicenseManagementServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan akses keLayanan AWS dan Sumber Daya yang digunakan atau dikelola olehAWS Marketplace untuk manajemen lisensi.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, grup, grup, peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 03 Desember 2020, 08:33 UTC
- Waktu yang telah diedit: 03 Desember 2020 08.33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowLicenseManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "license-manager:ListReceivedGrants",
        "license-manager:ListDistributedGrants",
        "license-manager:GetGrant",
        "license-manager:CreateGrant",
        "license-manager:CreateGrantVersion",
        "license-manager:DeleteGrant",
        "license-manager:AcceptGrant"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSMarketplaceManageSubscriptions

`AWSMarketplaceManageSubscriptions`adalah kebijakanAWS terkelola yang: Memberikan kemampuan untuk berlangganan dan berhenti berlangganAWS Marketplace perangkat lunak

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMarketplaceManageSubscriptions` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 19 Januari 2023, 23.45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMarketplaceMeteringFullAccess

`AWSMarketplaceMeteringFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS Marketplace Metering.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMarketplaceMeteringFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 17 Maret 2016, 22:39 UTC
- Waktu yang telah diedit: 17 Maret 2016 22.39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:MeterUsage"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMarketplaceMeteringRegisterUsage

`AWSMarketplaceMeteringRegisterUsage`adalah kebijakanAWS terkelola yang: Memberikan izin untuk mendaftarkan sumber daya dan melacak penggunaan melalui LayananAWS Marketplace Metering.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMarketplaceMeteringRegisterUsage` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 21 November 2019, 01:17 UTC
- Waktu yang telah diedit: 21 November 2019 01.17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:RegisterUsage"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMarketplaceProcurementSystemAdminFullAccess

`AWSMarketplaceProcurementSystemAdminFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke semua tindakan administratif untuk integrasiAWS Marketplace eProcurement.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMarketplaceProcurementSystemAdminFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 25 Juni 2019, 13:07 UTC
- Waktu yang telah diedit: 25 Juni 2019, 13.07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSMarketplacePurchaseOrdersServiceRolePolicy

`AWSMarketplacePurchaseOrdersServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan akses untukAWS Marketplace layanan untuk membeli manajemen pesanan.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Kebijakan tidak dapat dilampirkan kebijakan ini ke pengguna, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup,

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 27 Oktober 2021, 15:12 UTC
- Waktu yang telah diedit: 27 Oktober 2021 15.12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMarketplaceRead-only

`AWSMarketplaceRead-only`adalah kebijakanAWS terkelola yang: Memberikan kemampuan untuk meninjauAWS Marketplace langganan

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMarketplaceRead-only` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 19 Januari 2023, 23.30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceRead-only`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Resource" : "*",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow"
    },
    {
      "Resource" : "*",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListBuilds",
```

```
        "aws-marketplace:DescribeBuilds",
        "iam:ListRoles",
        "iam:ListInstanceProfiles",
        "sns:GetTopicAttributes",
        "sns:ListTopics"
      ]
    },
    {
      "Resource" : "*",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSMarketplaceResaleAuthorizationServiceRolePolicy

`AWSMarketplaceResaleAuthorizationServiceRolePolicy`adalah kebijakan AWS terkelola yang: Mengaktifkan akses ke Layanan AWS dan Sumber Daya yang digunakan atau dikelola oleh AWS Marketplace untuk Otorisasi Penjualan Kembali.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 Maret 2024, 18:47 UTC
- Waktu telah diedit: 05 Maret 2024, 18:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMCreate",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ram:RequestedResourceType" : "aws-marketplace:Entity"
        },
```

```
        "ArnLike" : {
          "ram:ResourceArn" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/
ResaleAuthorization/*"
        },
        "Null" : {
          "ram:Principal" : "true"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMAssociate",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "Null" : {
          "ram:Principal" : "false"
        },
        "StringEquals" : {
          "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMAccept",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMGet",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ]
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsMarketplace",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:GetResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsMarketplaceDescribe",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceSellerFullAccess

`AWSMarketplaceSellerFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke semua operasi penjual di AWS Marketplace dan AWS layanan lainnya seperti manajemen AMI.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMarketplaceSellerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Juli 2019, 20:40 UTC
- Waktu yang telah diedit: 15 Maret 2024, 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MarketplaceManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace-management:uploadFiles",
        "aws-marketplace-management:viewMarketing",
        "aws-marketplace-management:viewReports",
        "aws-marketplace-management:viewSupport",
```

```
        "aws-marketplace-management:viewSettings",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListTasks",
        "aws-marketplace:DescribeTask",
        "aws-marketplace:UpdateTask",
        "aws-marketplace:CompleteTask",
        "aws-marketplace:GetSellerDashboard",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AgreementAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "AssetScanning",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VendorInsights",
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Sid" : "SellerSettings",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace-management:GetSellerVerificationDetails",
```

```
        "aws-marketplace-management:PutSellerVerificationDetails",
        "aws-marketplace-management:GetBankAccountVerificationDetails",
        "aws-marketplace-management:PutBankAccountVerificationDetails",
        "aws-marketplace-management:GetSecondaryUserVerificationDetails",
        "aws-marketplace-management:PutSecondaryUserVerificationDetails",
        "aws-marketplace-management:GetAdditionalSellerNotificationRecipients",
        "aws-marketplace-management:PutAdditionalSellerNotificationRecipients",
        "payments:GetPaymentInstrument",
        "payments:CreatePaymentInstrument",
        "tax:GetTaxInterview",
        "tax:PutTaxInterview",
        "tax:GetTaxInfoReportingDocument"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Support",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourcePolicyManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "resale-authorization.marketplace.amazonaws.com"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMarketplaceSellerProductsFullAccess

`AWSMarketplaceSellerProductsFullAccess`adalahAWSkebijakan terkelolabahwa: Menyediakan penjual akses penuh keAWS MarketplaceHalaman Manajemen Produk dan lainnyaAWSlayanan seperti manajemen AMI.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMarketplaceSellerProductsFullAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 02 Juli 2019, 21:06 UTC
- Waktu yang diedit:18 Juli 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess`

Versi kebijakan

Versi kebijakan: v7(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListTasks",
        "aws-marketplace:DescribeTask",
        "aws-marketplace:UpdateTask",
        "aws-marketplace:CompleteTask",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSMarketplaceSellerProductsReadOnly

`AWSMarketplaceSellerProductsReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan penjual akses hanya-baca ke halaman ProdukAWS Marketplace Manajemen.

Menggunakan kebijakan

Anda dapat melampirkan`AWSMarketplaceSellerProductsReadOnly` ke pengguna, grup, dan peran Anda.

Rincian

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 02 Juli 2019, 21:40 UTC
- Waktu penyuntingan: 19 November 2022, 00.08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListTasks",
        "aws-marketplace:DescribeTask",
        "ec2:DescribeImages",
```

```
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMediaConnectServicePolicy

`AWSMediaConnectServicePolicy`adalah kebijakanAWS terkelola yang: Kebijakan default yang memungkinkan akses keLayanan AWS dan Sumber Daya yang digunakan atau dikelola oleh MediaConnect.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan tidak dapat dilampirkan pada pengguna, atau peran tidak dapat dilampirkan pada pengguna, atau peran tidak dapat dilampirkan

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 03 April 2023, 22:11 UTC
- Waktu yang telah diedit: 03 April 2023, 22.11 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:DeleteService",
        "ecs:CreateService",
        "ecs:DescribeServices",
        "ecs:PutAttributes",
        "ecs:DeleteAttributes",
        "ecs:RunTask",
        "ecs:ListTasks",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:UpdateContainerInstancesState"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateCluster",
        "ecs:UpdateClusterSettings",
        "ecs:ListAttributes",
        "ecs:DescribeClusters",
        "ecs:DeregisterContainerInstance",
        "ecs:ListContainerInstances"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMediaTailorServiceRolePolicy

`AWSMediaTailorServiceRolePolicy`adalah kebijakanAWS terkelola yang: Mengaktifkan akses keAWS Sumber Daya yang digunakan atau dikelola oleh MediaTailor

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, grup, peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan

- Waktu pembuatan: 17 September 2021, 22:27 UTC
- Waktu yang telah diedit: 17 September 2021 22.27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:MediaTailor/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:MediaTailor/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMigrationHubDiscoveryAccess

`AWSMigrationHubDiscoveryAccess`adalah kebijakanAWS terkelola yang: Kebijakan memungkinkan AWSMigrationHubService untuk menelepon AWSApplicationDiscoveryService atas nama pelanggan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMigrationHubDiscoveryAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Agustus 2017, 13:30 UTC
- Waktu yang telah diedit: 06 Agustus 2020, 17.34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "dms:AddTagsToResource",
      "Resource" : [
        "arn:aws:dms:*:*:endpoint:*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMigrationHubDMSAccess

`AWSMigrationHubDMSAccess`adalah kebijakanAWS terkelola yang: Kebijakan untuk Database Migration Service untuk mengambil peran dalam akun pelanggan untuk memanggil Migration Hub

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMigrationHubDMSAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Agustus 2017, 14:00 UTC
- Waktu yang telah diedit: 07 Oktober 2019 17.51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:CreateProgressUpdateStream"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS"
    },
    {
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:DescribeMigrationTask",
        "mgh:DisassociateCreatedArtifact",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:AssociateDiscoveredResource",
        "mgh:DisassociateDiscoveredResource",
        "mgh:ListDiscoveredResources"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS/*"
    },
    {
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:GetHomeRegion"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMigrationHubFullAccess

`AWSMigrationHubFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan terkelola untuk menyediakan akses pelanggan ke Layanan Migration Hub

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMigrationHubFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 14 Agustus 2017, 14:02 UTC
- Waktu yang telah diedit: 19 Juni 2019, 21.14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubFullAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:*",
        "discovery:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:GetRole"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "continuousexport.discovery.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "migrationhub.amazonaws.com",
            "dmsintegration.migrationhub.amazonaws.com",
            "smsintegration.migrationhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus menghapus dan menghapus menghapus dan menghapus izin identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMigrationHubOrchestratorConsoleFullAccess

`AWSMigrationHubOrchestratorConsoleFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses terbatas ke AWS Migration Hub, AWS Application Discovery Service, Amazon Simple Storage Service, dan AWS Secrets Manager. Kebijakan ini juga memberikan akses penuh ke layanan AWS Migration Hub Orchestrator.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubOrchestratorConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 April 2022, 02:26 UTC
- Waktu telah diedit: 05 Desember 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHO",
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "S3MHO",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::migrationhub-orchestrator-*",
        "arn:aws:s3:::migrationhub-orchestrator-*/*"
      ]
    },
    {
      "Sid" : "ListSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Configuration",
```

```
      "Effect" : "Allow",
      "Action" : [
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations",
        "discovery:GetDiscoverySummary"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetHomeRegion",
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMListProfileRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Account",
      "Effect" : "Allow",
      "Action" : [
        "account:ListRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "migrationhub-orchestrator.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/migrationhub-
orchestrator.amazonaws.com/AWSServiceRoleForMigrationHubOrchestrator*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM

- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubOrchestratorInstanceRolePolicy

`AWSMigrationHubOrchestratorInstanceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini perlu dilampirkan untuk instans migrasi SAP dan MGN agar layanan kami dapat mengatur instans dengan mengunduh skrip dari S3 dan untuk mengambil nilai rahasia di dalam instans EC2.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMigrationHubOrchestratorInstanceRolePolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 20 April 2022, 02:43 UTC
- Waktu yang telah diedit: 20 April 2022, 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::migrationhub-orchestrator-*",
        "arn:aws:s3:::aws-migrationhub-orchestrator-*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMigrationHubOrchestratorPlugin

`AWSMigrationHubOrchestratorPlugin`adalah kebijakanAWS terkelola yang: Menyediakan akses terbatas ke Amazon Simple Storage Service,AWS Secrets Manager, dan tindakan terkait Plugin untukAWS Migration Hub Orchestrator.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMigrationHubOrchestratorPlugin` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 20 April 2022, 02:25 UTC
- Waktu yang telah diedit: 20 April 2022, 02:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-orchestrator-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : [
        "arn:aws:execute-api:*:*:*/prod/*/put-log-data",
        "arn:aws:execute-api:*:*:*/prod/*/put-metric-data"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:RegisterPlugin",
        "migrationhub-orchestrator:GetMessage",
        "migrationhub-orchestrator:SendMessage"
      ],
      "Resource" : "arn:aws:migrationhub-orchestrator:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMigrationHubOrchestratorServiceRolePolicy

`AWSMigrationHubOrchestratorServiceRolePolicy`adalah kebijakan AWS terkelola yang: Menyediakan izin yang diperlukan untuk Migration Hub Orchestrator untuk memigrasi dan memodernisasi beban kerja lokal Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 April 2022, 02:24 UTC
- Waktu telah diedit: 04 Maret 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationDiscoveryService",
      "Effect" : "Allow",
      "Action" : [
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LaunchWizard",
      "Effect" : "Allow",
      "Action" : [
```

```
        "launchwizard:ListProvisionedApps",
        "launchwizard:DescribeProvisionedApp",
        "launchwizard:ListDeployments",
        "launchwizard:GetDeployment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2instances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ec2MGNLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "mgn.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ec2LaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeLaunchTemplates"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "getHomeRegion",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "SSMcommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetCommandInvocation",
        "ssm:CancelCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunRemoteScript",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:s3:::aws-migrationhub-orchestrator-*",
        "arn:aws:s3:::migrationhub-orchestrator-*"
      ]
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "s3GetObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::migrationhub-orchestrator-*",
        "arn:aws:s3:::migrationhub-orchestrator-*/*"
      ]
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
```

```
        "events:DeleteRule",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/MigrationHubOrchestratorManagedRule*"
    },
    {
      "Sid" : "MGN",
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetReplicationConfiguration",
        "mgn:GetLaunchConfiguration",
        "mgn:StartCutover",
        "mgn:FinalizeCutover",
        "mgn:StartTest",
        "mgn:UpdateReplicationConfiguration",
        "mgn:DescribeSourceServers",
        "mgn:MarkAsArchived",
        "mgn:ChangeServerLifeCycleState"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ec2DescribeImportImage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImportImageTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "s3ListBucket",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : "migrationhub-orchestrator-vmie-*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

`AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`adalahAWSkebijakan terkelolabahwa: Memberikan akses penuh keAWSRuang Refactor Hub Migrasi dan lainnyaAWSlayanan terkait kecualiAWSGrup keamanan Transit Gateway dan EC2 tidak diperlukan saat menggunakan lingkungan tanpa jembatan jaringan. Kebijakan ini juga mengecualikan izin yang diperlukanAWSLambda danAWSSumber daya Access Manager karena mereka dapat scoped bawah berdasarkan tag.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 03 April 2023, 20:09 UTC
- Waktu yang diedit:20 Juli 2023, 15:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`

Versi kebijakan

Versi kebijakan: v2(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:UpdateRestApiPolicy"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

`AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`adalah sebuahAWSkebijakan terkelolaitu: Gunakan dalam peran layanan IAM diteruskan ke dokumen Otomasi SSM AWSRefactorSpaces-CreateResources untuk memberikan izin yang diperlukan untuk menjalankan otomatisasi. Kebijakan ini memberikan akses baca/tulis ke tag EC2 untuk melacak kemajuan otomatisasi. Ketika jembatan jaringan lingkungan Refactor Spaces diaktifkan, otomatisasi juga menambahkan grup keamanan lingkungan ke instans EC2 untuk mengizinkan lalu lintas dari layanan Refactor Spaces lain di lingkungan. Kebijakan ini juga memberikan akses ke parameter SSM tindakan pasca peluncuran Layanan Migrasi Aplikasi.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 Agustus 2023, 15:08 UTC
- Waktu yang diedit:Agustus 10, 2023, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`

Versi kebijakan

Versi kebijakan: v1(default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/refactor-spaces:ssm:optin" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/refactor-spaces:ssm:optin" : "true"
        },
```

```
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "refactor-spaces:ssm:environment-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai denganAWSkebijakan terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubRefactorSpacesFullAccess

`AWSMigrationHubRefactorSpacesFullAccess`adalahAWSkebijakan terkelolabahwa: Memberikan akses penuh keAWS MigrationHubRuang Refactor,AWS MigrationHubFitur konsol Refactor Spaces dan terkait lainnyaAWSlayanan kecuali izin yang diperlukan untukAWSLambda danAWSSumber daya Access Manager karena mereka dapat scoped bawah berdasarkan tag.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMigrationHubRefactorSpacesFullAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 29 November 2021, 07.12 UTC
- Waktu yang diedit:19 Juli 2023, 19:07 UTC

- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess`

Versi kebijakan

Versi kebijakan: v5(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTransitGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:DeleteTags"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:UpdateRestApiPolicy"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSMigrationHubRefactorSpacesServiceRolePolicy

`AWSMigrationHubRefactorSpacesServiceRolePolicy`adalahAWSkebijakan terkelolabahwa: Menyediakan akses keAWSSumber daya yang dikelola atau digunakan olehAWSMigrasi Hub Refactor Spaces.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 29 November 2021, 06.50 UTC
- Waktu yang diedit:20 Juli 2023, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:DeleteTags",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:PUT",
        "apigateway:POST",
        "apigateway:GET",
        "apigateway:PATCH",
        "apigateway:DELETE"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : "arn:aws:apigateway:*::/vpclinks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSMigrationHubSMSAccess

`AWSMigrationHubSMSAccess`adalah kebijakanAWS terkelola yang: Kebijakan untuk Layanan Migrasi Server untuk mengambil peran dalam akun pelanggan untuk memanggil Migration Hub

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMigrationHubSMSAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Agustus 2017, 13:57 UTC
- Waktu yang telah diedit: 07 Oktober 2019 18.01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:CreateProgressUpdateStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS"
    },
    {
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:DescribeMigrationTask",
        "mgh:DisassociateCreatedArtifact",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:NotifyMigrationTaskState",
```

```
        "mgh:PutResourceAttributes",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:AssociateDiscoveredResource",
        "mgh:DisassociateDiscoveredResource",
        "mgh:ListDiscoveredResources"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS/*"
    },
    {
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:GetHomeRegion"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMigrationHubStrategyCollector

`AWSMigrationHubStrategyCollector`adalah kebijakan AWS terkelola yang: Memberikan izin untuk mengizinkan komunikasi dengan layanan Rekomendasi Strategi Hub AWS Migrasi, akses baca/tulis ke bucket S3 yang terkait dengan layanan, akses Amazon API Gateway untuk mengunggah log dan metrik, akses AWS Secrets AWS Manager untuk mengambil kredensi, dan layanan terkait apa pun.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMigrationHubStrategyCollector` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Oktober 2021 20:15 UTC
- Waktu telah diedit: 05 Februari 2024, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHSRAllowS3Resources",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MHSRAllowS3ListBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MHSRAllowMetricsAndLogs",
      "Effect" : "Allow",
      "Action" : [
        "application-transformation:PutMetricData",
        "application-transformation:PutLogData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MHSRAllowExecuteAPI",
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : [
        "arn:aws:execute-api:*:*:*/prod/*/put-log-data",
        "arn:aws:execute-api:*:*:*/prod/*/put-metric-data"
      ]
    },
    {
      "Sid" : "MHSRAllowCollectorAPI",
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-strategy:RegisterCollector",
```

```
        "migrationhub-strategy:GetAntiPattern",
        "migrationhub-strategy:GetMessage",
        "migrationhub-strategy:SendMessage",
        "migrationhub-strategy:ListAntiPatterns",
        "migrationhub-strategy:ListJarArtifacts",
        "migrationhub-strategy:UpdateCollectorConfiguration"
      ],
      "Resource" : "arn:aws:migrationhub-strategy:*:*:*"
    },
    {
      "Sid" : "MHSRAllowSecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-strategy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSMigrationHubStrategyConsoleFullAccess

`AWSMigrationHubStrategyConsoleFullAccess`adalah kebijakanAWS terkelola yang: Memberikan akses penuh ke layanan Rekomendasi StrategiAWS Migration Hub dan akses keAWS layanan terkait melalui layananAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMigrationHubStrategyConsoleFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 19 Oktober 2021, 20:13 UTC
- Waktu yang telah diedit: 09 November 2022, 00.00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-strategy:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:GetDiscoverySummary",
        "discovery:DescribeTags",
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "migrationhub-strategy.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/migrationhub-
strategy.amazonaws.com/AWSMigrationHubStrategyServiceRolePolicy*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSMigrationHubStrategyServiceRolePolicy

`AWSMigrationHubStrategyServiceRolePolicy`adalah kebijakanAWS terkelola yang: Mengaktifkan akses keAWS Sumber Daya yang digunakan atau dikelola oleh layanan Rekomendasi StrategiAWS Migration Hub.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna,, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup,

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 Oktober 2021, 20:02 UTC
- Waktu yang telah diedit: 19 Oktober 2021 20.02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default adalah versi yang menentukan izin untuk kebijakan terkelak. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "permissionsForAds",
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "permissionsForS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMobileHub_FullAccess

`AWSMobileHub_FullAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini dapat dilampirkan ke Pengguna, Peran, atau Grup mana pun, untuk memberikan izin kepada pengguna untuk membuat, menghapus, dan memodifikasi proyek (danAWS sumber daya terkait mereka) diAWS Mobile Hub. Ini juga mencakup izin untuk menghasilkan dan mengunduh contoh kode sumber aplikasi seluler untuk setiap proyek Mobile Hub.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMobileHub_FullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 05 Januari 2016, 19:56 UTC
- Waktu yang telah diedit: 19 Desember 2019 23.15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_FullAccess`

Versi kebijakan

Versi kebijakan:v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "cloudfront:GetDistribution",
        "devicefarm:CreateProject",
        "devicefarm:ListJobs",
        "devicefarm:ListRuns",
        "devicefarm:GetProject",
        "devicefarm:GetRun",
        "devicefarm:ListArtifacts",
        "devicefarm:ListProjects",
        "devicefarm:ScheduleRun",
        "dynamodb:DescribeTable",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "iam:ListSAMLProviders",
        "lambda:ListFunctions",
        "sns:ListTopics",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetBot",
        "lex:GetBots",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "mobilehub:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
```

```
      "Resource" : "arn:aws:s3:::*/aws-my-sample-app*.zip"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*-mobilehub-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*-mobilehub-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMobileHub_ReadOnly

`AWSMobileHub_ReadOnly`adalah kebijakanAWS terkelola yang: Kebijakan ini dapat dilampirkan ke Pengguna, Peran, atau Grup mana pun, untuk memberikan izin kepada pengguna untuk membuat daftar dan melihat proyek diAWS Mobile Hub. Ini juga mencakup izin untuk menghasilkan dan mengunduh contoh kode sumber aplikasi seluler untuk setiap proyek Mobile Hub. Ini tidak memungkinkan pengguna untuk memodifikasi konfigurasi apapun untuk proyek Mobile Hub.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSMobileHub_ReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 05 Januari 2016, 19:55 UTC
- Waktu yang telah diedit: 23 Juli 2018 09.59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly`

Versi kebijakan

Versi kebijakan:v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "iam:ListSAMLProviders",
        "lambda:ListFunctions",
        "sns:ListTopics",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetBot",
        "lex:GetBots",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "mobilehub:ExportProject",
        "mobilehub:GenerateProjectParameters",
        "mobilehub:GetProject",
        "mobilehub:SynchronizeProject",
        "mobilehub:GetProjectSnapshot",
```

```
        "mobilehub:ListProjectSnapshots",
        "mobilehub:ListAvailableConnectors",
        "mobilehub:ListAvailableFeatures",
        "mobilehub:ListAvailableRegions",
        "mobilehub:ListProjects",
        "mobilehub:ValidateProject",
        "mobilehub:VerifyServiceRole",
        "mobilehub:DescribeBundle",
        "mobilehub:ExportBundle",
        "mobilehub:ListBundles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/aws-my-sample-app*.zip"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSMSKReplicatorExecutionRole

`AWSMSKReplicatorExecutionRole`adalah kebijakan AWS terkelola yang: Memberikan izin ke Amazon MSK Replicator untuk mereplikasi data antara MSK Cluster.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSMSKReplicatorExecutionRole` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Desember 2023, 00:07 UTC
- Waktu telah diedit: 06 Desember 2023, 00:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:Connect",
        "kafka-cluster:DescribeCluster",
        "kafka-cluster:AlterCluster",
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup",
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:cluster/*"
      ]
```

```
    },
    {
      "Sid" : "TopicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration",
        "kafka-cluster:AlterCluster"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:topic/*/*"
      ]
    },
    {
      "Sid" : "GroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:group/*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSNetworkFirewallServiceRolePolicy

`AWSNetworkFirewallServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan AWSNetworkFirewall untuk membuat dan mengelola sumber daya yang diperlukan untuk Firewall Anda.

Menggunakan kebijakan ini ini ini telah terkelar

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini tidak dapat dilampirkan kebijakan ini untuk pengguna,,,,,,,,,,,,,,

Rincian kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 November 2020, 17:17 UTC
- Waktu yang telah diedit: 30 Maret 2023, 17.19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan ini adalah versi yang menentukan versi yang menentukan versi default kebijakan ini. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON JSON JSON JSON JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
```

```
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "acm:DescribeCertificate",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroupResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "resource-groups.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSNetworkManagerCloudWANServiceRolePolicy

`AWSNetworkManagerCloudWANServiceRolePolicy`adalah kebijakanAWS terkelola yang: Izinkan NetworkManager untuk mengakses sumber daya yang terkait dengan Jaringan Inti Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Juli 2022, 12:17 UTC
- Waktu yang telah diedit: 12 Juli 2022, 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSNetworkManagerFullAccess

`AWSNetworkManagerFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon NetworkManager melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSNetworkManagerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 03 Desember 2019, 17:37 UTC
- Waktu yang telah diedit: 03 Desember 2019 07.37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "networkmanager:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "networkmanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSNetworkManagerReadOnlyAccess

`AWSNetworkManagerReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Amazon NetworkManager melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSNetworkManagerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 Desember 2019, 17:35 UTC
- Waktu yang telah diedit: 03 Desember 2019 17.35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:Describe*",
```

```
        "networkmanager:Get*",
        "networkmanager:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSNetworkManagerServiceRolePolicy

`AWSNetworkManagerServiceRolePolicy`adalah kebijakanAWS terkelola yang: Izinkan NetworkManager untuk mengakses sumber daya yang terkait dengan Jaringan Global Anda

Menggunakan kebijakan ini kebijakan ini kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran ini ke pengguna, grup, atau peran ini ke pengguna, grup, atau peran ini

detail kebijakan kebijakan kebijakan detail kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 03 Desember 2019, 14:03 UTC
- Waktu yang telah diedit: 27 Juli 2022, 19.41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v8 (default)

Versi default kebijakan kebijakan ini adalah versi yang menentukan izin kebijakan kebijakan kebijakan ini adalah versi default kebijakan ini adalah versi default kebijakan ini adalah versi yang menentukan izin kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON kebijakan JSON dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeLocations",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpcs",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeRegions",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:GetTransitGatewayPolicyTableEntries"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSOpsWorks_FullAccess

`AWSOpsWorks_FullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS OpsWorks.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSOpsWorks_FullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 22 Januari 2021, 16:29 UTC
- Waktu yang telah diedit: 22 Januari 2021 16.29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorks_FullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfiles",
        "iam:ListRoles",
        "iam:ListUsers",
        "opsworks:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "opsworks.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSOpsWorksCloudWatchLogs

`AWSOpsWorksCloudWatchLogs`adalah kebijakanAWS terkelola yang: Memungkinkan OpsWorks instance dengan integrasi CWLogs diaktifkan untuk mengirimkan log dan membuat grup log yang diperlukan

Menggunakan kebijakan

Anda dapat melampirkan`AWSOpsWorksCloudWatchLogs` ke pengguna, grup, dan peran Anda.

Rincian

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 Maret 2017, 17:47 UTC
- Waktu yang telah diedit: 30 Maret 2017 07.47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksCloudWatchLogs`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSOpsWorksCMInstanceProfileRole

`AWSOpsWorksCMInstanceProfileRole`adalah kebijakanAWS terkelola yang: Menyediakan akses S3 untuk instance yang diluncurkan oleh OpsWorks CM.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSOpsWorksCMInstanceProfileRole` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 November 2016, 09:48 UTC
- Waktu yang telah diedit: 23 April 2021 17.34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksCMInstanceProfileRole`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudformation:DescribeStackResource",
        "cloudformation:SignalResource"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-opsworks-cm-*",
      "Effect" : "Allow"
    },
    {
      "Action" : "acm:GetCertificate",
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : "secretsmanager:GetSecretValue",
```

```
      "Resource" : "arn:aws:secretsmanager:*:*:opsworks-cm!aws-opsworks-cm-secrets-*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSOpsWorksCMServiceRole

`AWSOpsWorksCMServiceRole`adalah kebijakanAWS terkelola yang: Kebijakan Peran Layanan yang akan digunakan untuk Membuat server OpsWorks CM.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSOpsWorksCMServiceRole` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 24 November 2016, 09:49 UTC
- Waktu yang telah diedit: 23 April 2021 17.32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSOpsWorksCMServiceRole`

Versi kebijakan

Versi kebijakan:v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::aws-opsworks-cm-*"
      ],
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteObject",
        "s3:DeleteBucket",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutObject",
        "s3:GetBucketTagging",
        "s3:PutBucketTagging"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Action" : [
        "tag:UntagResources",
        "tag:TagResources"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloudformation:stack-name" : "aws-opsworks-cm-*"
        }
      },
      "Action" : [
        "ssm:SendCommand"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:ssm:*::document/*",
        "arn:aws:s3:::aws-opsworks-cm-*"
      ],
      "Action" : [
        "ssm:SendCommand"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateImage",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeregisterImage",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
```

```
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RunInstances",
        "ec2:StopInstances"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "aws-opsworks-cm-*"
        }
      },
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:RebootInstances"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:opsworks-cm:*:*:server/*"
      ],
      "Action" : [
        "opsworks-cm:DeleteServer",
        "opsworks-cm:StartMaintenance"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/aws-opsworks-cm-*"
      ],
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
```

```
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateStack"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/aws-opsworks-cm-*",
        "arn:aws:iam::*:role/service-role/aws-opsworks-cm-*"
      ],
      "Action" : [
        "iam:PassRole"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "acm:DeleteCertificate",
        "acm:ImportCertificate"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:opsworks-cm!aws-opsworks-cm-secrets-*",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteTags",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSOpsWorksInstanceRegistration

`AWSOpsWorksInstanceRegistration`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk instans Amazon EC2 untuk mendaftar denganAWS OpsWorks tumpukan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSOpsWorksInstanceRegistration` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 Juni 2016, 14:23 UTC
- Waktu yang telah diedit: 03 Juni 2016 14.23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "opsworks:DescribeStackProvisioningParameters",
        "opsworks:DescribeStacks",
        "opsworks:RegisterInstance"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSOpsWorksRegisterCLI_EC2

`AWSOpsWorksRegisterCLI_EC2`adalah kebijakanAWS terkelola yang: Kebijakan untuk mengaktifkan pendaftaran instans EC2 melalui OpsWorks CLI

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSOpsWorksRegisterCLI_EC2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 18 Juni 2019, 15:56 UTC

- Waktu yang telah diedit: 18 Juni 2019 15.56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_EC2`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "opsworks:AssignInstance",
        "opsworks:CreateLayer",
        "opsworks:DeregisterInstance",
        "opsworks:DescribeInstances",
        "opsworks:DescribeStackProvisioningParameters",
        "opsworks:DescribeStacks",
        "opsworks:UnassignInstance"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSOpsWorksRegisterCLI_OnPremises

`AWSOpsWorksRegisterCLI_OnPremises`adalah kebijakanAWS terkelola yang: Kebijakan untuk mengaktifkan pendaftaran instans Lokal melalui OpsWorks CLI

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSOpsWorksRegisterCLI_OnPremises` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 18 Juni 2019, 15:33 UTC
- Waktu yang telah diedit: 18 Juni 2019 15.33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_OnPremises`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "opsworks:AssignInstance",
        "opsworks:CreateLayer",
        "opsworks:DeregisterInstance",
        "opsworks:DescribeInstances",
        "opsworks:DescribeStackProvisioningParameters",
        "opsworks:DescribeStacks",
        "opsworks:UnassignInstance"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateGroup",
        "iam:AddUserToGroup"
      ],
      "Resource" : [
        "arn:aws:iam::*:group/AWS/OpsWorks/OpsWorks-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateUser",
        "iam:CreateAccessKey"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/AWS/OpsWorks/OpsWorks-*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachUserPolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/AWS/OpsWorks/OpsWorks-*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSOrganizationsFullAccess

`AWSOrganizationsFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke AWS Organizations.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSOrganizationsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 November 2018, 20:31 UTC

- Waktu telah diedit: 06 Februari 2024, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsFullAccess",
      "Effect" : "Allow",
      "Action" : "organizations:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:PutAlternateContact",
        "account:DeleteAlternateContact",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:PutContactInformation",
        "account:ListRegions",
        "account:EnableRegion",
        "account:DisableRegion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "organizations.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSOrganizationsReadOnlyAccess

`AWSOrganizationsReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya-baca ke Organizations AWS .

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSOrganizationsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 November 2018, 20:32 UTC
- Waktu telah diedit: 06 Februari 2024, 17:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsReadOnlyAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:ListRegions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSOrganizationsServiceTrustPolicy

`AWSOrganizationsServiceTrustPolicy`adalah kebijakanAWS terkelola yang: Kebijakan untuk memungkinkanAWS Organizations berbagi kepercayaan dengan pihak lain yang disetujuiLayanan AWS untuk tujuan menyederhanakan konfigurasi pelanggan.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran baru.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Oktober 2017, 23:04 UTC
- Waktu yang telah diedit: 01 November 2017 06.01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDeletionOfServiceLinkedRoleForOrganizations",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/organizations.amazonaws.com/*"
      ]
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSOutpostsAuthorizeServerPolicy

`AWSOutpostsAuthorizeServerPolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin yang memungkinkan Anda menginstal server Outpost di jaringan lokal Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSOutpostsAuthorizeServerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 04 Januari 2023, 19:23 UTC
- Waktu yang telah diedit: 04 Januari 2023, 19.23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:StartConnection",
        "outposts:GetConnection"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSOutpostsServiceRolePolicy

`AWSOutpostsServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan Peran Tertaut Layanan untuk mengaktifkan akses keAWS sumber daya yang dikelola olehAWS Outposts

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 09 November 2020, 22:55 UTC
- Waktu yang telah diedit: 09 November 2020, 22.55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan default adalah versi yang menentukan izin untuk kebijakan default. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSPanoramaApplianceRolePolicy

`AWSPanoramaApplianceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan perangkat lunakAWS IoT padaAWS Panorama Appliance untuk mengunggah log ke Amazon CloudWatch.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSPanoramaApplianceRolePolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Desember 2020, 13:13 UTC
- Waktu yang telah diedit: 01 Desember 2020, 13.13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*"
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/panorama_device*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSPanoramaApplianceServiceRolePolicy

`AWSPanoramaApplianceServiceRolePolicy`adalah kebijakanAWS terkelola yang: MemungkinkanAWS Panorama Appliance untuk mengunggah log ke Amazon CloudWatch, dan untuk mendapatkan objek dari titik akses Amazon S3 yang dibuat untuk digunakan denganAWS Panorama.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSPanoramaApplianceServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 Oktober 2021, 12:14 UTC

- Waktu yang telah diedit: 17 Januari 2023, 21.32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDevicePutMetric",
```

```
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "PanoramaDeviceMetrics"
        }
      }
    },
    {
      "Sid" : "PanoramaDeviceS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3:::*-nodepackage-store-*",
        "arn:aws:s3:::*-application-payload-store-*",
        "arn:aws:s3:*:*:accesspoint/panorama*"
      ],
      "Condition" : {
        "StringLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menghapus dan menentukan
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSPanoramaFullAccess

`AWSPanoramaFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS Panorama

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSPanoramaFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Desember 2020, 13:12 UTC
- Waktu yang telah diedit: 12 Januari 2022, 21.21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPanoramaFullAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "panorama:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
```

```
        "s3:PutObjectAcl",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:panorama*",
        "arn:aws:secretsmanager:*:*:secret:Panorama*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "panorama.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
```

```
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "panorama.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSPanoramaGreengrassGroupRolePolicy

`AWSPanoramaGreengrassGroupRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan fungsiAWS Lambda pada AlatAWS Panorama untuk mengelola sumber daya di Panorama, mengunggah log dan metrik ke Amazon CloudWatch, dan mengelola objek dalam bucket yang dibuat untuk digunakan dengan Panorama.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSPanoramaGreengrassGroupRolePolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Desember 2020, 13:10 UTC
- Waktu yang telah diedit: 06 Januari 2021 19.30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucket*",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    },
    {
      "Sid" : "PanoramaCLoudWatchPutDashboard",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutDashboard",
      "Resource" : [
        "arn:aws:cloudwatch::*:dashboard/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaCloudWatchPutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "PanoramaGreenGrassCloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/greengrass/*"
    },
```

```
    {
      "Sid" : "PanoramaAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSPanoramaSageMakerRolePolicy

`AWSPanoramaSageMakerRolePolicy`adalah kebijakanAWS terkelola yang: SageMaker Memungkinkan Amazon mengelola objek dalam bucket yang dibuat untuk digunakan denganAWS Panorama.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSPanoramaSageMakerRolePolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Desember 2020, 13:13 UTC
- Waktu yang telah diedit: 01 Desember 2020, 13.13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSPanoramaServiceLinkedRolePolicy

`AWSPanoramaServiceLinkedRolePolicy`adalah kebijakanAWS terkelola yang: MemungkinkanAWS Panorama untuk mengelola sumber daya diAWS IoT,AWS Secrets Manager danAWS Panorama.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 Oktober 2021, 12:12 UTC
- Waktu yang telah diedit: 20 Oktober 2021 12.12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
```

```
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:AttachPrincipalPolicy",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreateCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreatePolicyAndVersionAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion",
        "iot:AttachPolicy"
      ],
```

```
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeJobExecution",
        "iot:CreateJob",
        "iot:DeleteJob"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:job/panorama*",
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:Describe*",
        "panorama:List*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
```

```
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:panorama*",
        "arn:aws:secretsmanager:*:*:secret:Panorama*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSPanoramaServiceRolePolicy

`AWSPanoramaServiceRolePolicy`adalah kebijakanAWS terkelola yang: MemungkinkanAWS Panorama mengelola sumber daya di Amazon S3,AWS IoT,AWS IoT GreenGrass,AWS Lambda, Amazon SageMaker, dan Amazon CloudWatch Logs, dan untuk meneruskan peran layanan keAWS IoT,AWS IoT GreenGrass, dan Amazon SageMaker.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSPanoramaServiceRolePolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Desember 2020, 13:14 UTC
- Waktu yang telah diedit: 01 Desember 2020 13.14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:AttachPrincipalPolicy",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreateCertificateAndPolicyAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreatePolicyVersionAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeJobExecution",
        "iot:CreateJob",
        "iot:DeleteJob"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:job/panorama*",
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "panorama:Describe*",
        "panorama:List*",
        "panorama:Get*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:DeleteBucket",
        "s3:ListBucket",
        "s3:GetBucket*",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIAMPassSageMakerRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaSageMakerRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaSageMakerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "PanoramaIAMPassGreengrassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaGreengrassGroupRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassGroupRole",
        "arn:aws:iam::*:role/AWSPanoramaGreengrassRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "greengrass.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PanoramaIAMPassIoTRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaApplianceRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaApplianceRole"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "iot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PanoramaGreenGrassAccess",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:AssociateRoleToGroup",
        "greengrass:AssociateServiceRoleToAccount",
        "greengrass:CreateResourceDefinition",
        "greengrass:CreateResourceDefinitionVersion",
```

```
        "greengrass:CreateCoreDefinition",
        "greengrass:CreateCoreDefinitionVersion",
        "greengrass:CreateDeployment",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:CreateGroup",
        "greengrass:CreateGroupCertificateAuthority",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateLoggerDefinition",
        "greengrass:CreateLoggerDefinitionVersion",
        "greengrass:CreateSubscriptionDefinition",
        "greengrass:CreateSubscriptionDefinitionVersion",
        "greengrass:DeleteCoreDefinition",
        "greengrass:DeleteFunctionDefinition",
        "greengrass:DeleteResourceDefinition",
        "greengrass:DeleteGroup",
        "greengrass:DeleteLoggerDefinition",
        "greengrass:DeleteSubscriptionDefinition",
        "greengrass:DisassociateRoleFromGroup",
        "greengrass:DisassociateServiceRoleFromAccount",
        "greengrass:GetAssociatedRole",
        "greengrass:GetConnectivityInfo",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetDeviceDefinition",
        "greengrass:GetDeviceDefinitionVersion",
        "greengrass:GetFunctionDefinition",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupCertificateAuthority",
        "greengrass:GetGroupCertificateConfiguration",
        "greengrass:GetGroupVersion",
        "greengrass:GetLoggerDefinition",
        "greengrass:GetLoggerDefinitionVersion",
        "greengrass:GetResourceDefinition",
        "greengrass:GetServiceRoleForAccount",
        "greengrass:GetSubscriptionDefinition",
        "greengrass:GetSubscriptionDefinitionVersion",
        "greengrass:ListCoreDefinitionVersions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeployments",
        "greengrass:ListDeviceDefinitionVersions",
        "greengrass:ListDeviceDefinitions",
```

```
        "greengrass:ListFunctionDefinitionVersions",
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroupCertificateAuthorities",
        "greengrass:ListGroupVersions",
        "greengrass:ListGroups",
        "greengrass:ListLoggerDefinitionVersions",
        "greengrass:ListLoggerDefinitions",
        "greengrass:ListSubscriptionDefinitionVersions",
        "greengrass:ListSubscriptionDefinitions",
        "greengrass:ResetDeployments",
        "greengrass:UpdateConnectivityInfo",
        "greengrass:UpdateCoreDefinition",
        "greengrass:UpdateDeviceDefinition",
        "greengrass:UpdateFunctionDefinition",
        "greengrass:UpdateGroup",
        "greengrass:UpdateGroupCertificateConfiguration",
        "greengrass:UpdateLoggerDefinition",
        "greengrass:UpdateSubscriptionDefinition",
        "greengrass:UpdateResourceDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaLambdaUsersFunctionAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:CreateCompilationJob",
```

```
        "sagemaker:DescribeCompilationJob",
        "sagemaker:StopCompilationJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/panorama*",
        "arn:aws:sagemaker:*:*:compilation-job/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListCompilationJobs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    },
    {
      "Sid" : "PanoramaCWLogsAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPolicy",
        "iot:CreateRoleAlias"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*",
        "arn:aws:iot:*:*:rolealias/panorama*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSPriceListServiceFullAccess

`AWSPriceListServiceFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Layanan DaftarAWS Harga.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSPriceListServiceFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 22 November 2017, 00:36 UTC
- Waktu yang telah diedit: 22 November 2017, 00:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Action" : [
        "pricing:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSPrivateCAAuditor

`AWSPrivateCAAuditor`adalah kebijakanAWS terkelola yang: Memberikan akses auditor ke Otoritas SertifikatAWS Pribadi

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSPrivateCAAuditor` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 14 Februari 2023, 18:33 UTC
- Waktu yang telah diedit: 14 Pebruari 2023, 18.33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAAuditor`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:CreateCertificateAuthorityAuditReport",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:GetPolicy",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSPrivateCAFullAccess

`AWSPrivateCAFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Otoritas SertifikatAWS Pribadi

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSPrivateCAFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 14 Februari 2023, 18:20 UTC
- Waktu yang telah diedit: 14 Februari 2023, 18.20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM yang menentukan izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSPrivateCAPrivilegedUser

`AWSPrivateCAPrivilegedUser`adalah kebijakanAWS terkelola yang: Menyediakan akses pengguna sertifikat istimewa ke Otoritas SertifikatAWS Pribadi

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSPrivateCAPrivilegedUser` ke pengguna, grup, dan peran Anda.

detail

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 14 Februari 2023, 18:26 UTC
- Waktu yang telah diedit: 14 Februari 2023, 18.26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAPrivilegedUser`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSPrivateCAReadOnly

`AWSPrivateCAReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Otoritas SertifikatAWS Pribadi

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSPrivateCAReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 14 Februari 2023, 18:30 UTC
- Waktu yang telah diedit: 14 Februari 2023, 18.30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAReadOnly`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:ListCertificateAuthorities",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:GetPolicy",
      "acm-pca:ListPermissions",
      "acm-pca:ListTags"
    ],
    "Resource" : "*"
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSPrivateCAUser

`AWSPrivateCAUser`adalah kebijakanAWS terkelola yang: Menyediakan akses pengguna sertifikat ke Otoritas SertifikatAWS Pribadi

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSPrivateCAUser` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 14 Februari 2023, 18:16 UTC
- Waktu yang telah diedit: 14 Februari 2023, 18.16 UTC

- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAUser`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSPrivateMarketplaceAdminFullAccess

`AWSPrivateMarketplaceAdminFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke semua tindakan administratif untuk Marketplace AWS Pribadi.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSPrivateMarketplaceAdminFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 27 November 2018, 16:32 UTC
- Waktu yang telah diedit: 14 Februari 2024, 22:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateMarketplaceRequestPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:AssociateProductsWithPrivateMarketplace",
        "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCatalogAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceCatalogTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Sid" : "PrivateMarketplaceOrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSPrivateMarketplaceRequests

`AWSPrivateMarketplaceRequests`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk membuat permintaan di MarketplaceAWS Pribadi.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSPrivateMarketplaceRequests` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 28 Oktober 2019, 21:44 UTC
- Waktu yang telah diedit: 28 Oktober 2019 21.44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSPrivateNetworksServiceRolePolicy

`AWSPrivateNetworksServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Layanan JaringanAWS Pribadi untuk mengelola sumber daya atas nama pelanggan.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 16 Desember 2021, 23:17 UTC
- Waktu yang telah diedit: 16 Desember 2021 02.07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSProtonCodeBuildProvisioningBasicAccess

`AWSProtonCodeBuildProvisioningBasicAccess`adalah kebijakanAWS terkelola yang: Izin CodeBuild perlu menjalankan build untukAWS Proton CodeBuild Provisioning.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSProtonCodeBuildProvisioningBasicAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 November 2022, 21:04 UTC

- Waktu yang telah diedit: 09 November 2022, 21.04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/AWSProton-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "proton:NotifyResourceDeploymentStatusChange",
      "Resource" : "arn:aws:proton:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSProtonCodeBuildProvisioningServiceRolePolicy

`AWSProtonCodeBuildProvisioningServiceRolePolicy`adalah kebijakanAWS terkelola yang: MemungkinkanAWS Proton untuk mengelola penyediaan sumber daya Proton menggunakanCodeBuild danAWS layanan lainnya atas nama Anda.

Menggunakan kebijakan ini kebijakan ini kebijakan ini kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran ini.

detail kebijakan rincian kebijakan rincian kebijakan rincian

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 09 November 2022, 21:32 UTC
- Waktu yang telah diedit: 17 Mei 2023, 16:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default versi kebijakan ini adalah versi yang menentukan izin untuk kebijakan ini. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan SON SON SON SON SON SON SON SON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
```

```
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ListStackResources"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AWSProton-CodeBuild-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:UpdateProject",
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:RetryBuild",
        "codebuild:BatchGetBuilds",
        "codebuild:BatchGetProjects"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/AWSProton*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "codebuild.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSProtonDeveloperAccess

`AWSProtonDeveloperAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses ke APIAWS Proton dan Konsol Manajemen, tetapi tidak mengizinkan administrasi templat atau lingkungan Proton.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSProtonDeveloperAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 17 Februari 2021, 19:02 UTC
- Waktu yang telah diedit: 18 November 2022, 18.35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonDeveloperAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codestar-connections:ListConnections",
        "codestar-connections:UseConnection",
        "proton:CancelServiceInstanceDeployment",
        "proton:CancelServicePipelineDeployment",
        "proton:CreateService",
        "proton:DeleteService",
        "proton:GetAccountRoles",
        "proton:GetAccountSettings",
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
        "proton:GetEnvironmentTemplateMinorVersion",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
        "proton:GetResourcesSummary",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentOutputs",
        "proton:ListEnvironmentProvisionedResources",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplateMajorVersions",
        "proton:ListEnvironmentTemplateMinorVersions",
        "proton:ListEnvironmentTemplates",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListRepositories",
        "proton:ListRepositorySyncDefinitions",
        "proton:ListServiceInstanceOutputs",
```

```
        "proton:ListServiceInstanceProvisionedResources",
        "proton:ListServiceInstances",
        "proton:ListServicePipelineOutputs",
        "proton:ListServicePipelineProvisionedResources",
        "proton:ListServices",
        "proton:ListServiceTemplateMajorVersions",
        "proton:ListServiceTemplateMinorVersions",
        "proton:ListServiceTemplates",
        "proton:ListServiceTemplateVersions",
        "proton:ListTagsForResource",
        "proton:UpdateService",
        "proton:UpdateServiceInstance",
        "proton:UpdateServicePipeline",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSProtonFullAccess

`AWSProtonFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke APIAWS Proton dan Konsol Manajemen. Selain izin ini, akses ke Amazon S3 juga diperlukan untuk mendaftarkan bundel template dari bucket S3 Anda, serta akses ke Amazon IAM untuk membuat dan mengelola peran layanan untuk Proton.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSProtonFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 17 Februari 2021, 19:07 UTC
- Waktu yang telah diedit: 20 Juni 2022, 12.36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "proton:*",
        "codestar-connections:ListConnections",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "proton.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "proton.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sync.proton.amazonaws.com/
AWSServiceRoleForProtonSync",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "sync.proton.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:PassConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "codestar-connections:PassedToService" : "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSProtonReadOnlyAccess

`AWSProtonReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke APIAWS Proton dan Konsol Manajemen.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSProtonReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 17 Februari 2021, 19:09 UTC
- Waktu yang telah diedit: 18 November 2022, 18.28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "proton:GetAccountRoles",
        "proton:GetAccountSettings",
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
        "proton:GetEnvironmentTemplateMinorVersion",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
        "proton:GetResourcesSummary",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentOutputs",
        "proton:ListEnvironmentProvisionedResources",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplateMajorVersions",
        "proton:ListEnvironmentTemplateMinorVersions",
        "proton:ListEnvironmentTemplates",
```

```
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListRepositories",
        "proton:ListRepositorySyncDefinitions",
        "proton:ListServiceInstanceOutputs",
        "proton:ListServiceInstanceProvisionedResources",
        "proton:ListServiceInstances",
        "proton:ListServicePipelineOutputs",
        "proton:ListServicePipelineProvisionedResources",
        "proton:ListServices",
        "proton:ListServiceTemplateMajorVersions",
        "proton:ListServiceTemplateMinorVersions",
        "proton:ListServiceTemplates",
        "proton:ListServiceTemplateVersions",
        "proton:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSProtonServiceGitSyncServiceRolePolicy

`AWSProtonServiceGitSyncServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan yang memungkinkanAWS Proton untuk menyinkronkan definisi layanan, lingkungan, dan komponen Anda dari repositori git Anda keAWS Proton.

Menggunakan kebijakan ini.

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini tidak dapat melampirkan kebijakan ini tidak dapat melampirkan kebijakan ini tidak dapat dilampirkan kebijakan ini tidak dapat dilampirkan

Kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 04 April 2023, 15:55 UTC
- Waktu yang telah diedit: 04 April 2023, 15.55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi standar kebijakan ini adalah versi yang mengizinkan kebijakan untuk kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan yang mengizinkan kebijakan kebijakan kebijakan kebijakan yang mengizinkan kebijakan kebijakan kebijakan kebijakan kebijakan yang mengizinkan kebijakan kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonServiceSync",
      "Effect" : "Allow",
      "Action" : [
        "proton:GetService",
        "proton:UpdateService",
        "proton:UpdateServicePipeline",
        "proton:GetServiceInstance",
        "proton:CreateServiceInstance",
        "proton:UpdateServiceInstance",
        "proton:ListServiceInstances",
        "proton:GetComponent",
        "proton:CreateComponent",
```

```
        "proton:ListComponents",
        "proton:UpdateComponent",
        "proton:GetEnvironment",
        "proton:CreateEnvironment",
        "proton:ListEnvironments",
        "proton:UpdateEnvironment"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSProtonSyncServiceRolePolicy

`AWSProtonSyncServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan yang memungkinkanAWS Proton untuk menyinkronkan isi repositori git Anda ke Proton atau menyinkronkan konten Proton ke repositori git Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 November 2021, 21:14 UTC
- Waktu yang telah diedit: 23 November 2021 09.14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SyncToProton",
      "Effect" : "Allow",
      "Action" : [
        "proton:UpdateServiceTemplateVersion",
        "proton:UpdateServiceTemplate",
        "proton:UpdateEnvironmentTemplateVersion",
        "proton:UpdateEnvironmentTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:GetServiceTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetEnvironmentTemplate",
        "proton:DeleteServiceTemplateVersion",
        "proton:DeleteEnvironmentTemplateVersion",
        "proton:CreateServiceTemplateVersion",
        "proton:CreateServiceTemplate",
        "proton:CreateEnvironmentTemplateVersion",
        "proton:CreateEnvironmentTemplate",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListServiceTemplateVersions",
        "proton:CreateEnvironmentTemplateMajorVersion",
        "proton:CreateServiceTemplateMajorVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
```

```
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSPurchaseOrdersServiceRolePolicy

`AWSPurchaseOrdersServiceRolePolicy`adalahAWSkebijakan terkelolabahwa: Memberikan izin untuk melihat dan memodifikasi pesanan pembelian di konsol penagihan

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSPurchaseOrdersServiceRolePolicy`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 06 Mei 2020, 18:15 UTC
- Waktu yang diedit:17 Juli 2023, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v5(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetContactInformation",
        "aws-portal:*Billing",
        "consolidatedbilling:GetAccountBillingRole",
        "invoicing:GetInvoicePDF",
        "payments:GetPaymentInstrument",
        "payments:ListPaymentPreferences",
        "purchase-orders:AddPurchaseOrder",
        "purchase-orders:DeletePurchaseOrder",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "purchase-orders:ModifyPurchaseOrders",
        "purchase-orders:TagResource",
        "purchase-orders:UntagResource",
        "purchase-orders:UpdatePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrderStatus",
        "purchase-orders:ViewPurchaseOrders",
        "tax:ListTaxRegistrations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSQuicksightAthenaAccess

`AWSQuicksightAthenaAccess`adalah kebijakanAWS terkelola yang: Akses cepat ke bucket Athena API dan S3 yang digunakan untuk hasil kueri Athena

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSQuicksightAthenaAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 Desember 2016, 02:31 UTC
- Waktu yang telah diedit: 07 Juli 2021 20.09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess`

Versi kebijakan

Versi kebijakan:v10 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetQueryExecution",
        "athena:CancelQueryExecution",
        "athena:GetCatalogs",
        "athena:GetExecutionEngine",
        "athena:GetExecutionEngines",
        "athena:GetNamespace",
        "athena:GetNamespaces",
        "athena:GetQueryExecution",
```

```
        "athena:GetQueryExecutions",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetTable",
        "athena:GetTables",
        "athena:ListQueryExecutions",
        "athena:RunQuery",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:ListWorkGroups",
        "athena:ListEngineVersions",
        "athena:GetWorkGroup",
        "athena:GetDataCatalog",
        "athena:GetDatabase",
        "athena:GetTableMetadata",
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
```

```
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-athena-query-results-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSQuickSightDescribeRDS

`AWSQuickSightDescribeRDS`adalah kebijakanAWS terkelola yang: Izinkan QuickSight untuk menggambarkan sumber daya RDS

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSQuickSightDescribeRDS` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 November 2015, 23:24 UTC
- Waktu yang telah diedit: 10 November 2015 02.24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSQuickSightDescribeRedshift

`AWSQuickSightDescribeRedshift`adalah kebijakanAWS terkelola yang: Izinkan QuickSight untuk menjelaskan sumber daya Redshift

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSQuickSightDescribeRedshift` ke pengguna, grup, dan peran Anda.

detail kebijakan kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 November 2015, 23:25 UTC
- Waktu yang telah diedit: 10 November 2015 02.25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "redshift:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSQuickSightElasticsearchPolicy

`AWSQuickSightElasticsearchPolicy`adalah kebijakanAWS terkelola yang: Menyediakan akses ke sumber daya Amazon Elasticsearch dari Amazon QuickSight

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSQuickSightElasticsearchPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 09 September 2020, 17:27 UTC
- Waktu yang telah diedit: 07 September 2021 02.07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/",
        "arn:aws:es:*:*:domain/*/_cluster/settings",
        "arn:aws:es:*:*:domain/*/_cat/indices"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "es:ListDomainNames",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:DescribeElasticsearchDomain",
        "es:DescribeDomain"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpPost",
```

```
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/_opendistro/_sql",
        "arn:aws:es:*:*:domain/*/_plugin/_sql"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSQuickSightIoTAnalyticsAccess

`AWSQuickSightIoTAnalyticsAccess`adalah kebijakanAWS terkelola yang: Berikan akses QuickSight hanya-baca ke kumpulan data IoT Analytics

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSQuickSightIoTAnalyticsAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 November 2017, 17:00 UTC
- Waktu yang telah diedit: 29 November 2017, 17.00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iotanalytics:ListDatasets",
        "iotanalytics:DescribeDataset",
        "iotanalytics:GetDatasetContent"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSQuickSightListIAM

`AWSQuickSightListIAM`adalah kebijakanAWS terkelola yang: Izinkan QuickSight untuk mencantumkan entitas IAM

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSQuickSightListIAM` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 10 November 2015, 23:25 UTC
- Waktu yang telah diedit: 10 November 2015 02.25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSQuicksightOpenSearchPolicy

`AWSQuicksightOpenSearchPolicy`adalah kebijakanAWS terkelola yang: Menyediakan akses ke OpenSearch sumber daya Amazon dari Amazon QuickSight

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSQuicksightOpenSearchPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 07 September 2021, 23:26 UTC
- Waktu yang telah diedit: 07 September 2021 07.26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/",
        "arn:aws:es:*:*:domain/*/_cluster/settings",
        "arn:aws:es:*:*:domain/*/_cat/indices"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "es:ListDomainNames",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:DescribeDomain"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpPost",
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/_opendistro/_sql",
        "arn:aws:es:*:*:domain/*/_plugin/_sql"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan dan dan menghapus izin identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSQuickSightSageMakerPolicy

`AWSQuickSightSageMakerPolicy`adalah kebijakan AWS terkelola yang: Menyediakan akses ke SageMaker sumber daya Amazon dari Amazon QuickSight

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSQuickSightSageMakerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 17 Januari 2020, 17:18 UTC
- Waktu yang telah diedit: 30 Oktober 2023, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerTransformJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:CreateTransformJob"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:transform-job/quicksight-auto-generated-*"
    },
    {
      "Sid" : "SageMakerModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListModels",
```

```
        "sagemaker:DescribeModel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ObjectReadAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::quicksight-ml.*",
        "arn:aws:s3:::sagemaker*"
      ]
    },
    {
      "Sid" : "S3ObjectUpdateAccess",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : "arn:aws:s3:::sagemaker*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3BucketReadAccess",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::sagemaker*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSQuickSightTimestreamPolicy

`AWSQuickSightTimestreamPolicy`adalah kebijakanAWS terkelola yang:AWS QuickSight akses keAWS Timestream API. Pelanggan dapat melampirkan kebijakan ini keAWS QuickSight peran untuk memungkinkan pengambilan data dan metadata.

Menggunakan kebijakan

Anda dapat melampirkan`AWSQuickSightTimestreamPolicy` ke pengguna, grup, dan peran Anda.

detail

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 30 September 2020, 21:47 UTC
- Waktu yang telah diedit: 30 September 2020 21.47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:Select",
        "timestream:CancelQuery",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
```

```
        "timestream:DescribeTable",
        "timestream:DescribeDatabase",
        "timestream:SelectValues",
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Mendan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSReachabilityAnalyzerServiceRolePolicy

`AWSReachabilityAnalyzerServiceRolePolicy`adalah kebijakan AWS terkelola yang: Memungkinkan VPC Reachability Analyzer untuk mengakses AWS sumber daya dan berintegrasi dengan AWS Organisasi atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 November 2022, 17:12 UTC
- Waktu yang telah diedit: 23 Juni 2023, 21.04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
```

```
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "tag:GetResources",
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSRefactoringToolkitFullAccess

`AWSRefactoringToolkitFullAccess`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin untuk menggunakan AWS layanan dengan ekstensi AWS Toolkit for .NET Refactoring untuk Microsoft Visual Studio. Ini dimaksudkan untuk dilampirkan ke AWS profil lokal. Kebijakan ini memungkinkan mengunggah artefak aplikasi dan mengunduh artefak yang dihasilkan dari Amazon S3. Ini memungkinkan membangun aplikasi ke dalam gambar kontainer menggunakan AWS CodeBuild dan menyimpan dan mengambil gambar dari Amazon Elastic Container Registry (Amazon ECR). Dan itu memungkinkan penyebaran aplikasi ke layanan kontainer AWS seperti Amazon Elastic Container Service (Amazon ECS), pembuatan sumber daya VPC opsional, koneksi opsional ke infrastruktur yang ada seperti AWS Directory Service, dan layanan terkait lainnya.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSRefactoringToolkitFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 25 Oktober 2022, 16:41 UTC
- Waktu telah diedit: 18 November 2023, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "App2ContainerAccess",
      "Effect" : "Allow",
      "Action" : [
        "a2c:GetContainerizationJobDetails",
        "a2c:GetDeploymentJobDetails",
        "a2c:StartContainerizationJob",
        "a2c:StartDeploymentJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ExecuteChangeSet",
```

```
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:*:cloudformation:*:*:stack/a2c-app-*",
        "arn:*:cloudformation:*:*:stack/a2c-build-*",
        "arn:*:cloudformation:*:*:stack/application-transformation-app-*"
      ]
    },
    {
      "Sid" : "CodeBuildCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:UpdateProject"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "CodeBuildExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:StartBuild"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/*"
    },
    {
      "Sid" : "CreateSecurityGroupAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2CreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
```

```
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2CreateAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2ModifyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteTags",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
```

```
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2ModifyAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteTags",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcrCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "EcrCreateAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcrModifyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetLifecyclePolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "EcrModifyAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetLifecyclePolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
```

```
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcsCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:CreateService",
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "EcsCreateAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:CreateService",
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcsModifyAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "EcsModifyAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcsReadTaskDefinitionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTaskDefinition"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EcsExecuteCommandInSidecar",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:ExecuteCommand"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "a2c-sidecar"
        }
      }
    },
    {
      "Sid" : "EcsExecuteCommandInSidecarATS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ExecuteCommand"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "application-transformation-sidecar"
        }
      }
    },
    {
      "Sid" : "CreateEcsServiceLinkedRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudwatchCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
```

```
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "a2c-generated"
          ]
        }
      }
    },
    {
      "Sid" : "CloudwatchCreateAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "application-transformation"
          ]
        }
      }
    },
    {
      "Sid" : "CloudwatchGetAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
```

```
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "CloudwatchGetAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "SsmParameterAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:GetParameters",
        "ssm:PutParameter",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/a2c-generated-check-ecs-slr-*"
    },
    {
      "Sid" : "SsmMessagesAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
```

```
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/refactoringtoolkit*",
        "arn:aws:s3:::*/a2c-generated*",
        "arn:aws:s3:::*/application-transformation*"
      ]
    },
    {
      "Sid" : "S3ListAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "application-transformation",
            "refactoringtoolkit"
          ]
        }
      }
    },
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "clouddirectory:ListDirectories",
        "codebuild:BatchGetProjects",
        "codebuild:BatchGetBuilds",
        "ds:DescribeDirectories",
```

```
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ecr:DescribeImages",
        "ecr:DescribeRepositories",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTasks",
        "ecs:ListTagsForResource",
        "ecs:ListTasks",
        "iam:ListRoles",
        "s3:GetBucketLocation",
        "s3:GetBucketVersioning",
        "s3:ListAllMyBuckets",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetECSSLR",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS"
    },
    {
      "Sid" : "PortingAssistantFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore",
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore/*"
      ]
    },
```

```
    {
      "Sid" : "ApplicationTransformationAccess",
      "Effect" : "Allow",
      "Action" : [
        "application-transformation:StartPortingCompatibilityAssessment",
        "application-transformation:GetPortingCompatibilityAssessment",
        "application-transformation:StartPortingRecommendationAssessment",
        "application-transformation:GetPortingRecommendationAssessment",
        "application-transformation:PutLogData",
        "application-transformation:PutMetricData",
        "application-transformation:StartContainerization",
        "application-transformation:GetContainerization",
        "application-transformation:StartDeployment",
        "application-transformation:GetDeployment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
    },
    {
      "Sid" : "EcrPushAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer"
      ],
```

```
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "ecr:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcrAuthAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSRefactoringToolkitSidecarPolicy

`AWSRefactoringToolkitSidecarPolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini dimaksudkan untuk digunakan oleh Tugas Amazon ECS yang dibuat untuk menguji aplikasi dalamAWS menggunakan ekstensiAWS Toolkit for .NET Refactoring untuk Microsoft Visual Studio. Kebijakan ini memberikan akses untuk mengunduh artefak aplikasi dari Amazon S3, mengomunikasikan status Tugas menggunakanAWS Systems Manager, dan layanan lain yang diperlukan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSRefactoringToolkitSidecarPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 25 Oktober 2022, 16:41 UTC
- Waktu yang telah diedit: 29 Oktober 2022, 22.15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SsmMessagesAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssmmessages:OpenControlChannel",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssmmessages:CreateDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/refactoringtoolkit*"
    },
    {
      "Sid" : "S3ListBucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : "refactoringtoolkit*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSrePostPrivateCloudWatchAccess

`AWSrePostPrivateCloudWatchAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses Re:Post Private untuk mempublikasikan data metrik CloudWatch

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 15 November 2023, 16:37 UTC
- Waktu telah diedit: 15 November 2023, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchPublishMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/rePostPrivate",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSRepostSpaceSupportOperationsPolicy

`AWSRepostSpaceSupportOperationsPolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini memungkinkan layanan re:Post Space untuk membuat, mengelola, dan menyelesaikan kasus Support yang dibuat melalui aplikasi Space.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSRepostSpaceSupportOperationsPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 November 2023, 21:52 UTC
- Waktu telah diedit: 26 November 2023, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSResilienceHubAsssessmentExecutionPolicy

`AWSResilienceHubAsssessmentExecutionPolicy`adalah kebijakan AWS terkelola yang: Peran layanan Policy for AWS Resilience Hub yang memungkinkan akses ke AWS layanan lain untuk melaksanakan penilaian.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResilienceHubAsssessmentExecutionPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Juni 2023, 12:32 UTC
- Waktu telah diedit: 29 Oktober 2023, 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubFullResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ValidateTemplate",
        "cloudwatch:DescribeAlarms",
```

```
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "devops-guru:ListMonitoredResources",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "drs:DescribeJobs",
        "drs:DescribeSourceServers",
        "drs:GetReplicationConfiguration",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleets",
        "ec2:DescribeHosts",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ecr:DescribeRegistry",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
```

```
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:ListAliases",
        "lambda:ListVersionsByFunction",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSnapshots",
        "rds:DescribeGlobalClusters",
        "resource-groups:GetGroup",
        "resource-groups:ListGroupResources",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "s3:GetBucketLocation",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetMultiRegionAccessPointRoutes",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
```

```
        "servicecatalog:GetApplication",
        "servicecatalog:ListAssociatedResources",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "ssm:DescribeAutomationExecutions",
        "states:DescribeStateMachine",
        "states:ListStateMachineVersions",
        "states:ListStateMachineAliases",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSResilienceHubApiGatewayStatement",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans"
      ]
    },
    {
      "Sid" : "AWSResilienceHubS3Statement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::aws-resilience-hub-artifacts-*"
    },
    {
      "Sid" : "AWSResilienceHubCloudWatchStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "ResilienceHub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubSSMStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSResourceAccessManagerFullAccess

`AWSResourceAccessManagerFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS Resource Access Manager

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSResourceAccessManagerFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 04 Juni 2019, 17:28 UTC

- Waktu yang telah diedit: 04 Juni 2019 07.28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSResourceAccessManagerReadOnlyAccess

`AWSResourceAccessManagerReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca keAWS Resource Access Manager.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSResourceAccessManagerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 Desember 2019, 20:58 UTC
- Waktu yang telah diedit: 09 Desember 2019 20.58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:Get*",
        "ram:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSResourceAccessManagerResourceShareParticipantAccess

`AWSResourceAccessManagerResourceShareParticipantAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses ke APIAWS Resource Access Manager yang dibutuhkan oleh peserta berbagi sumber daya.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSResourceAccessManagerResourceShareParticipantAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 Desember 2019, 20:41 UTC
- Waktu yang telah diedit: 09 Desember 2019 08.41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourcePolicies",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShares",
        "ram:ListPendingInvitationResources",
        "ram:ListPrincipals",
        "ram:ListResources",
        "ram:RejectResourceShareInvitation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSResourceAccessManagerServiceRolePolicy

`AWSResourceAccessManagerServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan yang berisi aksesAWS Resource Access Manager Read-only ke struktur Organizations pelanggan. Hal ini juga berisi izin IAM untuk menghapus peran.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan

- Waktu pembuatan: 14 November 2018, 19:28 UTC
- Waktu yang telah diedit: 14 November 2018 07.28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDeletionOfServiceLinkedRoleForResourceAccessManager",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/aws-service-role/ram.amazonaws.com/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSResourceExplorerFullAccess

`AWSResourceExplorerFullAccess`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin administratif untuk mengakses sumber daya Resource Explorer dan memberikan izin hanya-baca ke layanan lain AWS untuk mendukung akses ini.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResourceExplorerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 November 2022, 20:01 UTC
- Waktu yang telah diedit: 14 November 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerConsoleFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceExplorerSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSResourceExplorerOrganizationsAccess

`AWSResourceExplorerOrganizationsAccess`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin administratif ke Resource Explorer dan memberikan izin hanya-baca ke layanan lain AWS untuk mendukung akses ini. Administrator AWS Organizations memerlukan izin ini untuk mengatur dan mengelola pencarian multi-akun di konsol.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResourceExplorerOrganizationsAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 14 November 2023, 17:01 UTC
- Waktu telah diedit: 14 November 2023, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
        "ec2:DescribeRegions",
        "ram:ListResources",
```

```
        "ram:GetResourceShares",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceExplorerGetSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer"
    },
    {
      "Sid" : "ResourceExplorerCreateSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationsAdministratorAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSResourceExplorerReadOnlyAccess

`AWSResourceExplorerReadOnlyAccess`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin hanya-baca untuk mencari dan melihat sumber daya Resource Explorer dan memberikan izin hanya-baca ke layanan lain untuk mendukung akses ini. AWS

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSResourceExplorerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 November 2022, 19:56 UTC
- Waktu telah diedit: 14 November 2023, 16:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:Get*",
        "resource-explorer-2:List*",
        "resource-explorer-2:Search",
        "resource-explorer-2:BatchGetView",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSResourceExplorerServiceRolePolicy

`AWSResourceExplorerServiceRolePolicy`adalah kebijakan AWS terkelola yang: Memungkinkan Resource Explorer melihat sumber daya dan CloudTrail peristiwa atas nama Anda untuk mengindeks sumber daya Anda untuk penelusuran.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 25 Oktober 2022, 20:35 UTC
- Waktu telah diedit: 20 Desember 2023, 13:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
```

```
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/resource-explorer-2/*"
      ]
    },
    {
      "Sid" : "ApiGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/deployments"
      ]
    },
    {
      "Sid" : "ResourceInventoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
        "acm-pca:ListCertificateAuthorities",
        "amplify:ListApps",
        "amplify:ListBackendEnvironments",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplifyuibuilder:ListComponents",
        "amplifyuibuilder:ListThemes",
        "app-integrations:ListEventIntegrations",
        "apprunner:ListServices",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeApplications",
        "appstream:DescribeFleets",
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
        "appsync:ListGraphqlApis",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListWorkspaces",
        "athena:ListDataCatalogs",
        "athena:ListWorkGroups",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:ListBackupPlans",
        "backup:ListReportPlans",
        "batch:DescribeComputeEnvironments",
```

```
        "batch:DescribeJobQueues",
        "batch:ListSchedulingPolicies",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudfront:ListCachePolicies",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListDistributions",
        "cloudfront:ListFieldLevelEncryptionConfigs",
        "cloudfront:ListFieldLevelEncryptionProfiles",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeInsightRules",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "codeartifact:ListDomains",
        "codeartifact:ListRepositories",
        "codebuild:ListProjects",
        "codecommit:ListRepositories",
        "codeguru-profiler:ListProfilingGroups",
        "codepipeline:ListPipelines",
        "codestar-connections:ListConnections",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:ListUserPools",
        "databrew:ListDatasets",
        "databrew:ListRecipes",
        "databrew:ListRulesets",
        "detective:ListGraphs",
        "ds:DescribeDirectories",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeElasticGpus",
```

```
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeFpgaImages",
        "ec2:DescribeHostReservations",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeImportSnapshotTasks",
        "ec2:DescribeInstanceEventWindows",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpams",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
```

```
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVerifiedAccessEndpoints",
        "ec2:DescribeVerifiedAccessGroups",
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessTrustProviders",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetSubnetCidrReservations",
        "ecr:DescribeRepositories",
        "ecr-public:DescribeRepositories",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeServices",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeReservedCacheNodes",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "emr-serverless:ListApplications",
        "es:ListDomainNames",
```

```
        "events:ListEventBuses",
        "events:ListRules",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "finspace:ListEnvironments",
        "firehose:ListDeliveryStreams",
        "fis:ListExperimentTemplates",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "frauddetector:GetDetectors",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetLabels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetVariables",
        "gamelift:ListAliases",
        "geo:ListPlaceIndexes",
        "geo:ListTrackers",
        "greengrass:ListComponents",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "glue:GetDatabases",
        "glue:GetJobs",
        "glue:GetTables",
        "glue:GetTriggers",
        "greengrass:ListComponentVersions",
        "greengrass:ListGroups",
        "healthlake:ListFHIRDatastores",
        "iam:ListGroups",
        "iam:ListInstanceProfiles",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
```

```
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iot:ListJobTemplates",
        "iot:ListAuthorizers",
        "iot:ListMitigationActions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListSecurityProfiles",
        "iot:ListThings",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListGateways",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListWorkspaces",
        "kafka:ListConfigurations",
        "kms:ListKeys",
        "ivs:ListChannels",
        "ivs:ListStreamKeys",
        "kafka:ListClusters",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kinesisvideo:ListStreams",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
```

```
        "lex:ListBots",
        "lex:ListBotAliases",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "lookoutmetrics:ListAlerts",
        "lookoutvision:ListProjects",
        "mediapackage:ListChannels",
        "mediapackage:ListOriginEndpoints",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mq:ListBrokers",
        "mediatailor:ListPlaybackConfigurations",
        "memorydb:DescribeACLs",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeUsers",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTemplates",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetDevices",
        "networkmanager:GetLinks",
        "networkmanager:ListAttachments",
        "networkmanager:ListCoreNetworks",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "panorama:ListPackages",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListLedgers",
        "rds:DescribeBlueGreenDeployments",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
```

```
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeReservedDBInstances",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeSnapshotSchedules",
        "redshift:DescribeUsageLimits",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "rekognition:DescribeProjects",
        "resiliencehub:ListApps",
        "resiliencehub:ListResiliencyPolicies",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListViews",
        "resource-groups:ListGroups",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverRules",
        "s3:GetBucketLocation",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListStorageLensConfigurations",
```

```
        "sagemaker:ListModels",
        "sagemaker:ListNotebookInstances",
        "secretsmanager:ListSecrets",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAttributeGroups",
        "signer:ListSigningProfiles",
        "sns:ListTopics",
        "sqs:ListQueues",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeMaintenanceWindowTargets",
        "ssm:DescribeMaintenanceWindowTasks",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
        "ssm-incidents:ListResponsePlans",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListInventoryEntries",
        "ssm:ListResourceDataSync",
        "states:ListActivities",
        "states:ListStateMachines",
        "timestream:ListDatabases",
        "wisdom:listAssistantAssociations",
        "wisdom:ListAssistants",
        "wisdom:listKnowledgeBases"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSResourceGroupsReadOnlyAccess

`AWSResourceGroupsReadOnlyAccess`adalah kebijakanAWS terkelola yang: Ini adalah kebijakan baca saja untukAWS Resource Groups

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSResourceGroupsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 07 Maret 2018, 10:27 UTC
- Waktu yang telah diedit: 05 Pebruari 2019, 17.56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "tag:Get*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeSnapshots",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListClusters",
        "glacier:ListVaults",
        "glacier:DescribeVault",
        "glacier:ListTagsForVault",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:ListTagsForStream",
        "opsworks:DescribeStacks",
        "opsworks:ListTags",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeTags",
        "route53domains:ListDomains",
        "route53:ListHealthChecks",
        "route53:GetHealthCheck",
        "route53:ListHostedZones",
        "route53:GetHostedZone",
        "route53:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListTagsForResource",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "ssm:ListDocuments"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSRoboMaker_FullAccess

`AWSRoboMaker_FullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS RoboMaker melaluiAWS Management Console dan SDK. Juga menyediakan akses pilih ke layanan terkait (misalnya, S3, IAM).

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSRoboMaker_FullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 10 September 2020, 18:34 UTC
- Waktu yang telah diedit: 16 September 2021 21.06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : "robomaker:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecr:BatchGetImage",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecr-public:DescribeImages",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSRoboMakerReadOnlyAccess

`AWSRoboMakerReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya bacaAWS RoboMaker melaluiAWS Management Console dan SDK

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSRoboMakerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 26 November 2018, 05:30 UTC
- Waktu yang telah diedit: 28 Agustus 2020, 23.10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSRoboMakerServicePolicy

`AWSRoboMakerServicePolicy`adalah kebijakanAWS terkelola yang: kebijakan RoboMaker layanan

Menggunakan

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan pada pengguna,,,,,,,,,,,,,,,,,,,,,,,,

Rincian

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 November 2018, 06:30 UTC
- Waktu yang telah diedit: 11 November 2021 22.23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default adalah versi yang menentukan izin yang mengizinkan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "greengrass:CreateDeployment",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetAssociatedRole",
        "lambda:CreateFunction",
        "robomaker:CreateSimulationJob",
```

```
        "robomaker:CancelSimulationJob"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "robomaker:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:robomaker:*:*:simulation-job/*"
    },
    {
      "Action" : [
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration",
        "lambda:DeleteFunction",
        "lambda:ListVersionsByFunction",
        "lambda:GetAlias",
        "lambda:UpdateAlias",
        "lambda:CreateAlias",
        "lambda:DeleteAlias"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:lambda:*:*:function:aws-robomaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "robomaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSRoboMakerServiceRolePolicy

`AWSRoboMakerServiceRolePolicy`adalah kebijakanAWS terkelola yang: kebijakan RoboMaker layanan

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSRoboMakerServiceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 26 November 2018, 05:33 UTC
- Waktu yang telah diedit: 26 November 2018 05.33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "greengrass:CreateDeployment",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetAssociatedRole",
        "lambda:CreateFunction"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:lambda:*:*:function:aws-robomaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSRolesAnywhereServicePolicy

`AWSRolesAnywhereServicePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Peran IAM Di Mana Saja untuk mempublikasikan metrik layanan/penggunaan CloudWatch dan memeriksa status Otoritas Sertifikat Pribadi atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 Juli 2022, 15:26 UTC
- Waktu yang telah diedit: 05 Juli 2022, 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan ini adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/RolesAnywhere",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSS3OnOutpostsServiceRolePolicy

`AWSS3OnOutpostsServiceRolePolicy`adalah kebijakan AWS terkelola yang: Izinkan layanan Amazon S3 on Outposts mengelola sumber daya jaringan EC2 atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 03 Oktober 2023, 20:32 UTC
- Waktu telah diedit: 03 Oktober 2023, 20:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:DescribeAddresses",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations"
      ],
      "Resource" : "*",
```

```
      "Sid" : "DescribeVpcResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Sid" : "CreateNetworkInterface"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "S3 On Outposts"
        }
      },
      "Sid" : "CreateTagsForCreateNetworkInterface"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:ipv4pool-ec2/*"
      ],
      "Sid" : "AllocateIpAddress"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "S3 On Outposts"
        }
      },
      "Sid" : "CreateTagsForAllocateIpAddress"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:AssociateAddress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "S3 On Outposts"
        }
      },
      "Sid" : "ReleaseVpcResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "AllocateAddress"
          ],
          "aws:RequestTag/CreatedBy" : [
            "S3 On Outposts"
          ]
        }
```

```
      },
      "Sid" : "CreateTags"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSavingsPlansFullAccess

`AWSSavingsPlansFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke layanan Savings Plans

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSSavingsPlansFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 November 2019, 22:45 UTC
- Waktu yang telah diedit: 06 November 2019 02.45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "savingsplans:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSSavingsPlansReadOnlyAccess

`AWSSavingsPlansReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke layanan Savings Plans

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSSavingsPlansReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 November 2019, 22:45 UTC
- Waktu yang telah diedit: 06 November 2019 02.45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "savingsplans:Describe*",
        "savingsplans:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSSecurityHubFullAccess

`AWSSecurityHubFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh untuk menggunakan AWS Security Hub.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSecurityHubFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola

- Waktu pembuatan: 27 November 2018, 23:54 UTC
- Waktu telah diedit: 16 November 2023, 21:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubAllowAll",
      "Effect" : "Allow",
      "Action" : "securityhub:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "securityhub.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OtherServicePermission",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:GetDetector",
        "guardduty:ListDetectors",
        "inspector2:BatchGetAccountStatus"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSecurityHubOrganizationsAccess

`AWSSecurityHubOrganizationsAccess`adalah kebijakan AWS terkelola yang: Memberikan izin untuk mengaktifkan dan mengelola AWS Security Hub dalam suatu organisasi. Termasuk mengaktifkan layanan di seluruh organisasi, dan menentukan akun administrator yang didelegasikan untuk layanan.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSecurityHubOrganizationsAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 15 Maret 2021, 20:53 UTC
- Waktu yang telah diedit: 16 November 2023, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubOrganizationsAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationPermissionsEnable",
      "Effect" : "Allow",
      "Action" : "organizations:EnableAWSServiceAccess",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "securityhub.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OrganizationPermissionsDelegatedAdmin",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
```

```
      "Resource" : "arn:aws:organizations::*:account/o-*/*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "securityhub.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSecurityHubReadOnlyAccess

`AWSSecurityHubReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses baca saja ke sumber daya AWS Security Hub

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSecurityHubReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 November 2018, 01:34 UTC
- Waktu telah diedit: 22 Februari 2024, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSecurityHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:Get*",
        "securityhub:List*",
        "securityhub:BatchGet*",
        "securityhub:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSecurityHubServiceRolePolicy

`AWSSecurityHubServiceRolePolicy`adalah kebijakan AWS terkelola yang: Peran terkait layanan yang diperlukan untuk AWS Security Hub untuk mengakses sumber daya Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 27 November 2018, 23:47 UTC
- Waktu telah diedit: 27 November 2023, 03:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v14 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "logs:DescribeMetricFilters",
        "sns:ListSubscriptionsByTopic",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
```

```
        "config:DescribeConfigRules",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:BatchGetResourceConfig",
        "config:SelectResourceConfig",
        "iam:GenerateCredentialReport",
        "organizations:ListAccounts",
        "config:PutEvaluations",
        "tag:GetResources",
        "iam:GetCredentialReport",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "securityhub:BatchDisableStandards",
        "securityhub:BatchEnableStandards",
        "securityhub:BatchUpdateStandardsControlAssociations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:CreateMembers",
        "securityhub:DeleteMembers",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeStandards",
        "securityhub:DescribeStandardsControls",
        "securityhub:DisassociateFromAdministratorAccount",
        "securityhub:DisassociateMembers",
        "securityhub:DisableSecurityHub",
        "securityhub:EnableSecurityHub",
        "securityhub:GetEnabledStandards",
        "securityhub:ListStandardsControlAssociations",
        "securityhub:ListSecurityControlDefinitions",
        "securityhub:UpdateOrganizationConfiguration",
        "securityhub:UpdateSecurityControl",
        "securityhub:UpdateSecurityHubConfiguration",
        "securityhub:UpdateStandardsControl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceRoleConfigPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
```

```
        "config:DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
    },
    {
      "Sid" : "SecurityHubServiceRoleOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceCatalogAdminFullAccess

`AWSServiceCatalogAdminFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke kemampuan admin katalog layanan

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSServiceCatalogAdminFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 15 Februari 2018, 17:19 UTC
- Waktu yang telah diedit: 13 April 2023, 18.43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess`

Versi kebijakan

Versi kebijakan:v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListStackResources",
        "cloudformation:TagResource",
        "cloudformation:CreateStackSet",
        "cloudformation:CreateStackInstances",
        "cloudformation:UpdateStackSet",
        "cloudformation:UpdateStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
```

```
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateUploadBucket",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ValidateTemplate",
        "iam:GetGroup",
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "servicecatalog:Get*",
        "servicecatalog:Scan*",
        "servicecatalog:Search*",
        "servicecatalog:List*",
        "servicecatalog:TagResource",
        "servicecatalog:UntagResource",
        "servicecatalog:SyncResource",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:Accept*",
```

```
        "servicecatalog:Associate*",
        "servicecatalog:Batch*",
        "servicecatalog:Copy*",
        "servicecatalog:Create*",
        "servicecatalog:Delete*",
        "servicecatalog:Describe*",
        "servicecatalog:Disable*",
        "servicecatalog:Disassociate*",
        "servicecatalog:Enable*",
        "servicecatalog:Execute*",
        "servicecatalog:Import*",
        "servicecatalog:Provision*",
        "servicecatalog:Put*",
        "servicecatalog:Reject*",
        "servicecatalog:Terminate*",
        "servicecatalog:Update*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "servicecatalog.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
orgsdatasync.servicecatalog.amazonaws.com/AWSServiceRoleForServiceCatalogOrgsDataSync",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "orgsdatasync.servicecatalog.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSServiceCatalogAdminReadOnlyAccess

`AWSServiceCatalogAdminReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke kemampuan admin Service Catalog

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSServiceCatalogAdminReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 25 Oktober 2019, 18:53 UTC
- Waktu yang telah diedit: 25 Oktober 2019 18.53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "iam:GetGroup",
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "servicecatalog:Get*",
        "servicecatalog:List*",
        "servicecatalog:Describe*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:Search*",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus dihapus
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSServiceCatalogAppRegistryFullAccess

`AWSServiceCatalogAppRegistryFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke kemampuan Service Catalog App Registry

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSServiceCatalogAppRegistryFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 12 November 2020, 22:25 UTC
- Waktu telah diedit: 07 Desember 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppRegistryUpdateStackAndResourceGroupTagging",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack",
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRegistryResourceGroupsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "resource-groups:GetGroup",
        "resource-groups:GetTags",
        "resource-groups:Tag",
        "resource-groups:Untag",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:AssociateResource",
        "resource-groups:DisassociateResource"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/AWS_*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AppRegistryServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRegistryOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "servicecatalog:CreateApplication",
        "servicecatalog:GetApplication",
        "servicecatalog:UpdateApplication",
        "servicecatalog:DeleteApplication",
        "servicecatalog:ListApplications",
        "servicecatalog:AssociateResource",
        "servicecatalog:DisassociateResource",
        "servicecatalog:GetAssociatedResource",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup",
        "servicecatalog:ListAssociatedAttributeGroups",
        "servicecatalog:CreateAttributeGroup",
        "servicecatalog:UpdateAttributeGroup",
        "servicecatalog:DeleteAttributeGroup",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:SyncResource",
        "servicecatalog:ListAttributeGroupsForApplication",
        "servicecatalog:GetConfiguration",
        "servicecatalog:PutConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AppRegistryResourceTagging",
```

```
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListTagsForResource",
        "servicecatalog:UntagResource",
        "servicecatalog:TagResource"
      ],
      "Resource" : "arn:aws:servicecatalog:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceCatalogAppRegistryReadOnlyAccess

`AWSServiceCatalogAppRegistryReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke capabilites Service Catalog App Registry

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSServiceCatalogAppRegistryReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 12 November 2020
- Waktu yang telah diedit: 17 November 2022, 18.16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:GetApplication",
        "servicecatalog:ListApplications",
        "servicecatalog:GetAssociatedResource",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAssociatedAttributeGroups",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListTagsForResource",
        "servicecatalog:ListAttributeGroupsForApplication",
        "servicecatalog:GetConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSServiceCatalogAppRegistryServiceRolePolicy

`AWSServiceCatalogAppRegistryServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Service Catalog AppRegistry untuk mengelola Resource Groups atas nama Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 Mei 2021, atau 22:18 UTC
- Waktu yang telah diedit: 26 Oktober 2022, 16.05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:DescribeStacks",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:DeleteGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:GetTags",
        "resource-groups:Tag",
        "resource-groups:Untag"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration"
      ],
      "Resource" : [
        "arn:*:resource-groups:*:*:group/AWS_AppRegistry*",
        "arn:*:resource-groups:*:*:group/AWS_CloudFormation_Stack*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSServiceCatalogEndUserFullAccess

`AWSServiceCatalogEndUserFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke kemampuan enduser katalog layanan

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSServiceCatalogEndUserFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 15 Februari 2018, 17:22 UTC
- Waktu yang telah diedit: 10 Juli 2019, 20.30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess`

Versi kebijakan

Versi kebijakan:v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:ValidateTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DeleteChangeSet",
        "cloudformation:TagResource",
        "cloudformation:CreateStackSet",
        "cloudformation:CreateStackInstances",
        "cloudformation:UpdateStackSet",
        "cloudformation:UpdateStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:ProvisionProduct",
        "servicecatalog:SearchProducts",
```

```
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DescribeProvisionedProduct",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:ListStackInstancesForProvisionedProduct",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:CreateProvisionedProductPlan",
        "servicecatalog:DescribeProvisionedProductPlan",
        "servicecatalog:ExecuteProvisionedProductPlan",
        "servicecatalog:DeleteProvisionedProductPlan",
        "servicecatalog:ListProvisionedProductPlans",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:ExecuteProvisionedProductServiceAction",
        "servicecatalog:DescribeServiceActionExecutionParameters"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas
- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSServiceCatalogEndUserReadOnlyAccess

`AWSServiceCatalogEndUserReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke kemampuan pengguna akhir Service Catalog

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSServiceCatalogEndUserReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 25 Oktober 2019, 18:49 UTC
- Waktu yang telah diedit: 25 Oktober 2019 18.49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
```

```
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:SearchProducts",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DescribeProvisionedProduct",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:ListStackInstancesForProvisionedProduct",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:DescribeProvisionedProductPlan",
        "servicecatalog:ListProvisionedProductPlans",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:DescribeServiceActionExecutionParameters"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

`AWSServiceCatalogOrgsDataSyncServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan Peran Tertaut LayananAWS ServiceCatalog untuk disinkronkan dengan strukturAWS Organizations Organisasi

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 April 2023, 20:48 UTC
- Waktu yang telah diedit: 10 April 2023, 20.48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSServiceCatalogSyncServiceRolePolicy

`AWSServiceCatalogSyncServiceRolePolicy`adalah kebijakanAWS terkelola yang: Peran Tertaut LayananAWS ServiceCatalog untuk menyinkronkan Artefak Penyediaan dari repositori sumber

Menggunakan di atas.

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan ke pengguna,,,,,, peran, atau peran baru.

Perincian

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 15 November 2022, 21:20 UTC
- Waktu yang telah diedit: 15 November 2022, 21.20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Kebijakan ini dilampirkan ke atas nama. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

JSON SON SON SON SON SON SON SON SON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListProvisioningArtifacts",
        "servicecatalog:DescribeProductAsAdmin",
        "servicecatalog:DeleteProvisioningArtifact",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:DescribeProvisioningArtifact",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:UpdateProvisioningArtifact"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AccessArtifactRepositories",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "ValidateTemplate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSServiceRoleForAmazonEKSNodegroup

`AWSServiceRoleForAmazonEKSNodegroup`adalah kebijakan AWS terkelola yang: Izin diperlukan untuk mengelola nodegroup di akun pelanggan. Kebijakan ini terkait dengan pengelolaan sumber daya berikut: AutoscalingGroups, SecurityGroups, LaunchTemplates dan InstanceProfiles.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan

- Waktu pembuatan: 07 November 2019, 01:34 UTC
- Waktu telah diedit: 04 Januari 2024, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SharedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks" : "*"
        }
      }
    },
    {
      "Sid" : "EKSCreatedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
```

```
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "LaunchTemplateRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "AutoscalingRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:PutLifecycleHook",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:EnableMetricsCollection"
      ],
      "Resource" : "arn:aws:autoscaling:*:*:*:autoScalingGroupName/eks-*"
    },
    {
      "Sid" : "AllowAutoscalingToCreateSLR",
      "Effect" : "Allow",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      },
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowASGCreationByEKS",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:CreateAutoScalingGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToAutoscaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
```

```
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToManageResourcesForNodegroups",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "ec2:CreateLaunchTemplate",
        "ec2:DescribeInstances",
        "iam:GetInstanceProfile",
        "ec2:DescribeLaunchTemplates",
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:RunInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:GetConsoleOutput",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsToCreateAndManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks-*"
    },
    {
      "Sid" : "PermissionsToManageEKSAndKubernetesTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

`AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`adalah kebijakanAWS terkelola yang: Menyediakan akses ke sumber daya Systems Manager yang digunakan oleh CloudWatch Alarm

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna,,,,,,,,,,,,,,,,,, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 01 Oktober 2020, 09:49 UTC
- Waktu yang telah diedit: 01 Oktober 2020 09.49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePoli

`AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`adalah sebuahAWSkebijakan terkelolaitu: Memungkinkan CloudWatch untuk mengakses metrik RDS Performance Insights atas nama Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 September 2023, 09:32 UTC
- Waktu yang diedit:September 07, 2023, 09:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1(default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber dayaAWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai denganAWSkebijakan terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForCodeGuru-Profiler

`AWSServiceRoleForCodeGuru-Profiler`adalah kebijakanAWS terkelola yang: Peran terkait layanan yang diperlukan untuk Amazon CodeGuru Profiler untuk mengirim pemberitahuan atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, grup, atau peran baru.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 Juni 2020, 22:04 UTC
- Waktu yang telah diedit: 26 Juni 2020, 22.04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSNSPublishToSendNotifications",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSServiceRoleForCodeWhispererPolicy

`AWSServiceRoleForCodeWhispererPolicy`adalah kebijakan AWS terkelola yang: Peran ini memberikan izin CodeWhisperer untuk mengakses data di akun Anda untuk menghitung penagihan, menyediakan akses untuk membuat dan mengakses laporan keamanan di Amazon CodeGuru, dan memancarkan data ke akun Anda. CloudWatch

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 Maret 2023, 19:39 UTC
- Waktu telah diedit: 01 Maret 2024, 23:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid2",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListDirectoryAssociations",
        "sso:DescribeRegisteredRegions",
        "sso:GetProfile",
        "sso:GetManagedApplicationInstance",
        "sso:ListApplicationAssignments",
        "sso:DescribeInstance"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid3",
      "Effect" : "Allow",
```

```
      "Action" : [
        "codeguru-security:CreateUploadUrl"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid4",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:GetScan",
        "codeguru-security:ListFindings",
        "codeguru-security:GetFindings"
      ],
      "Resource" : [
        "arn:aws:codeguru-security:*:*:scans/CodeWhisperer-*"
      ]
    },
    {
      "Sid" : "sid5",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/CodeWhisperer"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForEC2ScheduledInstances

`AWSServiceRoleForEC2ScheduledInstances`adalah kebijakanAWS terkelola yang: Memungkinkan Instans Terjadwal EC2 untuk meluncurkan dan mengelola instans spot.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Oktober 2017, 18:31 UTC
- Waktu yang telah diedit: 12 Oktober 2017 18.31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
```

```
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:ec2sri:scheduledInstanceId"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2sri:scheduledInstanceId" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

`AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`adalah kebijakanAWS terkelola yang:AWS GroundStation menggunakan peran terkait layanan ini untuk memanggil EC2 untuk menemukan alamat IPv4 publik

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 13 Desember 2022, 23:52 UTC
- Waktu yang telah diedit: 13 Desember 2022, 23.52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan ini adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSServiceRoleForImageBuilder

`AWSServiceRoleForImageBuilder`adalah kebijakan AWS terkelola yang: Memungkinkan EC2 ImageBuilder memanggil AWS layanan atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 29 November 2019, 22:02 UTC
- Waktu yang telah diedit: 19 Oktober 2023, 21:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder`

Versi kebijakan

Versi kebijakan: v19 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
```

```
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "vmie.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CreateLaunchTemplate",
        "ec2:DeregisterImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeSnapshots",
        "ec2:DescribeHosts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateImage"
          ],
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:export-image-task/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
```

```
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "ssm:AddTagsToResource",
        "ssm:DescribeInstanceInformation",
        "ssm:GetAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListInventoryEntries",
        "ssm:SendAutomationSignal",
        "ssm:DescribeInstanceAssociationsStatus",
        "ssm:DescribeAssociationExecutions",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
        "arn:aws:ssm:*:*:document/AWS-RunShellScript",
        "arn:aws:ssm:*:*:document/AWSEC2-RunSysprep",
        "arn:aws:s3:::*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/CreatedBy" : [
            "EC2 Image Builder"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:StartAutomationExecution",
      "Resource" : "arn:aws:ssm:*:*:automation-definition/ImageBuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/EC2ImageBuilderDistributionCrossAccountRole"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DescribeLaunchTemplates",
        "ec2:ModifyLaunchTemplate",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : "arn:aws:ec2:*:*:export-image-task/*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CancelExportTask"
      ],
      "Resource" : "arn:aws:ec2:*:*:export-image-task/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ssm.amazonaws.com",
            "ec2fastlaunch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector2:ListCoverage",
        "inspector2:ListFindings"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:TagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/image-builder-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchDeleteImage"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/image-builder-*",
      "Condition" : {
        "StringEquals" : {
          "ecr:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
```

```
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/ImageBuilder-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForIoTSiteWise

`AWSServiceRoleForIoTSiteWise`adalah kebijakan AWS terkelola yang: Memungkinkan AWS IoT SiteWise untuk menyediakan dan mengelola gateway serta data kueri. Kebijakan ini mencakup izin AWS Greengrass yang diperlukan untuk diterapkan ke grup, izin AWS Lambda untuk membuat dan memperbarui fungsi awalan layanan, dan izin IoT Analytics untuk kueri data dari datastores. AWS

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 November 2018, 19:19 UTC
- Waktu telah diedit: 13 November 2023, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSiteWiseReadGreenGrass",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:GetAssociatedRole",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLog",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*:log-stream:*"
```

```
    },
    {
      "Sid" : "AllowSiteWiseAccessSiteWiseManagedWorkspaceInTwinMaker",
      "Effect" : "Allow",
      "Action" : [
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ExecuteQuery"
      ],
      "Resource" : "arn:aws:iottwinmaker:*:*:workspace/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iottwinmaker:linkedServices" : [
            "IOTSITEWISE"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForLogDeliveryPolicy

`AWSServiceRoleForLogDeliveryPolicy`adalah kebijakanAWS terkelola yang: Memungkinkan layanan Pengiriman Log untuk mengirimkan log dengan memanggil tujuan log atas nama Anda.

Menggunakan kebijakan terkait kebijakan terkait kebijakan terkait kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran baru.

detail kebijakan kebijakan kebijakan kebijakan JSON

- Tipe: Kebijakan peran terkait layanan

- Waktu pembuatan: 04 Oktober 2019, 17:31 UTC
- Waktu yang telah diedit: 15 Juli 2021 20.07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default default JSON adalah versi yang menentukan izin untuk kebijakan default JSON. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LogDeliveryEnabled" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSServiceRoleForMonitronPolicy

`AWSServiceRoleForMonitronPolicy`adalah kebijakanAWS terkelola yang: Memberikan izin Amazon Monitron untuk mengelolaAWS sumber daya, termasuk penetapan penggunaAWS SSO atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna,,,,,,,,,,,,,,,,, atau peran Anda.

detail kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 02 Desember 2020, 19:06 UTC
- Waktu yang telah diedit: 29 September 2022 20.38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan default kebijakan ini adalah versi yang menentukan izin untuk kebijakan default kebijakan ini. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "sso:GetManagedApplicationInstance",
        "sso:GetProfile",
        "sso:ListProfiles",
        "sso:ListProfileAssociations",
        "sso:AssociateProfile",
        "sso:ListDirectoryAssociations",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSServiceRoleForNeptuneGraphPolicy

`AWSServiceRoleForNeptuneGraphPolicy`adalah kebijakan AWS terkelola yang: Menyediakan akses Cloudwatch untuk mempublikasikan metrik operasional dan penggunaan serta log untuk Amazon Neptunus

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 29 November 2023, 14:03 UTC
- Waktu telah diedit: 29 November 2023, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GraphMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Neptune",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Sid" : "GraphLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/neptune/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "GraphLogEvents",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForPrivateMarketplaceAdminPolicy

`AWSServiceRoleForPrivateMarketplaceAdminPolicy`adalah kebijakan AWS terkelola yang: Menyediakan izin untuk mendeskripsikan dan memperbarui sumber daya Marketplace Pribadi dan menjelaskan AWS Organizations

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 14 Februari 2024, 22:28 UTC
- Waktu telah diedit: 14 Februari 2024, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateMarketplaceCatalogDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Audience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProcurementPolicy/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/BrandingSettings/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCatalogDescribeChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceCatalogListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceStartChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : [
            "AssociateAudience",
            "DisassociateAudience"
          ]
        }
      },
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceOrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListChildren"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSServiceRoleForSMS

`AWSServiceRoleForSMS`adalah kebijakanAWS terkelola yang: Menyediakan akses keAWS layanan dan sumber daya yang diperlukan untuk memigrasi instans layananAWS termasuk EC2, S3, dan Cloudformation.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 06 Agustus 2019, 18:39 UTC
- Waktu yang telah diedit: 15 Oktober 2020 17.28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS`

Versi kebijakan

Versi kebijakan:v10 (default)

Versi default Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*",
      "Condition" : {
        "Null" : {
          "cloudformation:ResourceTypes" : "false"
        },
        "ForAllValues:StringEquals" : {
          "cloudformation:ResourceTypes" : [
            "AWS::EC2::Instance",
            "AWS::ApplicationInsights::Application",
            "AWS::ResourceGroups::Group"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::sms-app-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:CreateReplicationJob",
        "sms:DeleteReplicationJob",
        "sms:GetReplicationJobs",
        "sms:GetReplicationRuns",
        "sms:GetServers",
        "sms:ImportServerCatalog",
        "sms:StartOnDemandReplicationRun",
        "sms:UpdateReplicationJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunRemoteScript",
        "arn:aws:s3:::sms-app-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/UseForSMSApplicationValidation" : [
```

```
            "true"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
```

```
          "ec2:ResourceTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DeregisterImage",
        "ec2:ImportImage",
        "ec2:DescribeImportImageTasks",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "cloudformation.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute",
        "ec2:StopInstances",
        "ec2:StartInstances",
```

```
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:CreateApplication",
        "applicationinsights:CreateComponent",
        "applicationinsights:UpdateApplication",
        "applicationinsights:DeleteApplication",
        "applicationinsights:UpdateComponentConfiguration",
        "applicationinsights:DeleteComponent"
      ],
      "Resource" : "arn:aws:applicationinsights:*:*:application/resource-group/sms-app-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:GetGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/sms-app-*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSServiceRolePolicyForBackupReports

`AWSServiceRolePolicyForBackupReports`adalah kebijakanAWS terkelola yang: Menyediakan izinAWS Backup untuk membuat laporan kepatuhan atas nama Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 Agustus 2021, 21:16 UTC
- Waktu yang telah diedit: 10 Maret 2023, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeFramework",
        "backup:ListBackupJobs",
        "backup:ListRestoreJobs",
        "backup:ListCopyJobs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:BatchGetResourceConfig",
        "config:SelectResourceConfig",
        "config:DescribeConfigurationAggregators",
        "config:SelectAggregateResourceConfig",
```

```
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/
backup.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigurationAggregator",
        "config:PutConfigurationAggregator"
      ],
      "Resource" : "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
backup.amazonaws.com*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSServiceRolePolicyForBackupRestoreTesting

`AWSServiceRolePolicyForBackupRestoreTesting`adalah kebijakan AWS terkelola yang: Kebijakan ini berisi izin untuk pengujian pemulihan dan untuk membersihkan sumber daya yang dibuat selama pengujian.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 November 2023, 23:37 UTC
- Waktu telah diedit: 14 Februari 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BackupActions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeRecoveryPoint",
        "backup:DescribeRestoreJob",
        "backup:DescribeProtectedResource",
        "backup:GetRecoveryPointRestoreMetadata",
        "backup:ListBackupVaults",
        "backup:ListProtectedResources",
        "backup:ListProtectedResourcesByBackupVault",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListRecoveryPointsByResource",
```

```
        "backup:ListTags",
        "backup:StartRestoreJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:TerminateInstances",
```

```
        "elasticfilesystem:DeleteFilesystem",
        "elasticfilesystem:DeleteMountTarget",
        "rds:DeleteDBCluster",
        "rds:DeleteDBInstance",
        "fsx:DeleteFileSystem",
        "fsx:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/awsbackup-restore-test" : "false"
        }
      }
    },
    {
      "Sid" : "DdbDeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/awsbackup-restore-test-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftDeleteActions",
      "Effect" : "Allow",
      "Action" : "redshift:DeleteCluster",
      "Resource" : "arn:aws:redshift:*:*:cluster:awsbackup-restore-test-*"
    },
    {
      "Sid" : "S3DeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::awsbackup-restore-test-*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TimestreamDeleteActions",
      "Effect" : "Allow",
      "Action" : "timestream:DeleteTable",
      "Resource" : "arn:aws:timestream:*:*:database/*/table/awsbackup-restore-test-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSShieldDRTAccessPolicy

`AWSShieldDRTAccessPolicy`adalah kebijakanAWS terkelola yang: Menyediakan Tim ResponsAWS DDoS akses terbatasAkun AWS ke Anda untuk membantu mitigasi serangan DDoS selama peristiwa tingkat keparahan tinggi.

Menggunakan kebijakan

Anda dapat melampirkan`AWSShieldDRTAccessPolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 05 Juni 2018, 22:29 UTC
- Waktu yang telah diedit: 15 Desember 2020, 17.28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SRTAccessProtectedResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:List*",
        "route53:List*",
        "elasticloadbalancing:Describe*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudfront:GetDistribution*",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:DescribeAccelerator",
        "ec2:DescribeRegions",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SRTManageProtections",
      "Effect" : "Allow",
      "Action" : [
        "shield:*",
        "waf:*",
        "wafv2:*",
        "waf-regional:*",
        "elasticloadbalancing:SetWebACL",
        "cloudfront:UpdateDistribution",
        "apigateway:SetWebACL"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSShieldServiceRolePolicy

`AWSShieldServiceRolePolicy`adalah kebijakanAWS terkelola yang: MemungkinkanAWS Shield mengaksesAWS sumber daya atas nama Anda untuk memberikan perlindungan DDoS.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 November 2021, 19:17 UTC
- Waktu yang telah diedit: 17 November 2021 19.17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSSSMForSAPServiceLinkedRolePolicy

`AWSSSMForSAPServiceLinkedRolePolicy`adalah kebijakan AWS terkelola yang: Menyediakan AWS Systems Manager untuk SAP dengan izin yang diperlukan untuk mengelola dan mengintegrasikan perangkat lunak SAP. AWS

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 16 November 2022, 01:18 UTC
- Waktu telah diedit: November 21, 2023, 03:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstanceStatus",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:DescribeInstanceStatus",
      "Resource" : "*"
    },
    {
      "Sid" : "TargetRuleActions",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:*:events:*:*:rule/SSMSAPManagedRule*",
        "arn:*:events:*:*:event-bus/default"
      ]
    },
    {
      "Sid" : "DocumentActions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:*:ssm:*:*:document/AWSSystemsManagerSAP-*",
        "arn:*:ssm:*:*:document/AWSSSMSAP*",
        "arn:*:ssm:*:*:document/AWSSAP*"
      ]
    },
    {
      "Sid" : "CustomerSendCommand",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ssm:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "InstanceTagActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/awsApplication" : "false"
        },
        "StringEqualsIgnoreCase" : {
          "ec2:ResourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "DescribeTag",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeTags",
      "Resource" : "*"
    },
    {
      "Sid" : "GetApplication",
      "Effect" : "Allow",
      "Action" : "servicecatalog:GetApplication",
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
    {
      "Sid" : "UpdateOrDeleteApplication",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DeleteApplication",
        "servicecatalog:UpdateApplication"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateApplication",
      "Effect" : "Allow",
```

```
      "Action" : [
        "servicecatalog:TagResource",
        "servicecatalog:CreateApplication"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:*:iam::*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Usage",
            "AWS/SSMForSAP"
          ]
        }
      }
    },
    {
      "Sid" : "CreateAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:CreateAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "GetAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:GetAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*"
    },
    {
      "Sid" : "DeleteAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:DeleteAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "AttributeGroupActions",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "ListAssociatedAttributeGroups",
      "Effect" : "Allow",
      "Action" : "servicecatalog:ListAssociatedAttributeGroups",
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
    {
      "Sid" : "CreateGroup",
      "Effect" : "Allow",
```

```
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SSMForSAPCreated"
          ]
        }
      }
    },
    {
      "Sid" : "GetGroup",
      "Effect" : "Allow",
      "Action" : "resource-groups:GetGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*"
    },
    {
      "Sid" : "DeleteGroup",
      "Effect" : "Allow",
      "Action" : "resource-groups:DeleteGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateAppTagResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "TagAppTagResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:Tag"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "GetAppTagResourceGroupConfig",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupConfiguration"
      ],
      "Resource" : [
        "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSSMOpsInsightsServiceRolePolicy

`AWSSSMOpsInsightsServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan untuk Peran Tertaut Layanan AWSServiceRoleForAmazonSSM_OpsInsights

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 16 Juni 2021, 20:12 UTC
- Waktu yang telah diedit: 16 Juni 2021 20.12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMOpsInsightsServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessOpsItem",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:UpdateOpsItem",
        "ssm:GetOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SsmOperationalInsight" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSSSODirectoryAdministrator

`AWSSSODirectoryAdministrator`adalah kebijakanAWS terkelola yang: Akses administrator untuk Direktori SSO

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSSSODirectoryAdministrator` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 31 Oktober 2018, 23:54 UTC
- Waktu yang telah diedit: 20 Oktober 2022, 20.34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSSSODirectoryReadOnly

`AWSSSODirectoryReadOnly`adalah kebijakanAWS terkelola yang: ReadOnly akses untuk Direktori SSO

Menggunakan kebijakan

Anda dapat melampirkan`AWSSSODirectoryReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 31 Oktober 2018, 23:49 UTC
- Waktu yang telah diedit: 16 November 2022, 18.17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:Search*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Get*",
        "identitystore:Describe*",
        "identitystore:List*",
        "identitystore-auth:ListSessions",
        "identitystore-auth:BatchGetSession"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSSSOMasterAccountAdministrator

`AWSSSOMasterAccountAdministrator`adalah kebijakanAWS terkelola yang: Menyediakan akses dalamAWS SSO untuk mengelola akun master dan anggotaAWS Organizations dan aplikasi cloud

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSSSOMasterAccountAdministrator` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Juni 2018, 20:36 UTC
- Waktu yang telah diedit: 20 Oktober 2022, 20.34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator`

Versi kebijakan

Versi kebijakan:v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "AWSSSOCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMasterAccountAdministrator",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeTrusts",
        "ds:UnauthorizeApplication",
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
```

```
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSSSOMemberAccountAdministrator

`AWSSSOMemberAccountAdministrator`adalah kebijakanAWS terkelola yang: Menyediakan akses dalamAWS SSO untuk mengelola akun anggotaAWS Organizations dan aplikasi cloud

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSSSOMemberAccountAdministrator` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Juni 2018, 20:45 UTC
- Waktu yang telah diedit: 20 Oktober 2022, 20.32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator`

Versi kebijakan

Versi kebijakan:v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListAccounts",
```

```
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSSSOReadOnly

`AWSSSOReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke konfigurasiAWS SSO.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSSSOReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Juni 2018, 20:24 UTC
- Waktu yang telah diedit: 22 Agustus 2022, 17:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOReadOnly`

Versi kebijakan

Versi kebijakan:v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren",
```

```
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso:Search*",
        "sso-directory:DescribeDirectory",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSSSOServiceRolePolicy

`AWSSSOServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memberikan izinAWS SSO untuk mengelolaAWS sumber daya, termasuk peran IAM, kebijakan, dan IdP SALL atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 Desember 2017, 18:36 UTC
- Waktu yang telah diedit: 20 Oktober 2022, 20.05 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v17 (default)

Versi standar kebijakan yang mengizinkan untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMRoleProvisioningActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription",
        "iam:UpdateAssumeRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:DeleteRolePermissionsBoundary"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMRoleReadActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
```

```
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMRoleCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ]
    },
    {
      "Sid" : "IAMSLRCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:DeleteRole",
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO"
      ]
    },
    {
      "Sid" : "IAMSAMLProviderCreationAction",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ],
      "Condition" : {
        "StringNotEquals" : {
```

```
          "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMSAMLProviderUpdateAction",
      "Effect" : "Allow",
      "Action" : [
        "iam:UpdateSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ]
    },
    {
      "Sid" : "IAMSAMLProviderCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSAMLProvider",
        "iam:GetSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowUnauthAppForDirectory",
      "Effect" : "Allow",
      "Action" : [
        "ds:UnauthorizeApplication"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeForDirectory",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeAndListOperationsOnIdentitySource",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "identitystore:DescribeGroup",
        "identitystore:ListGroups",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSStepFunctionsConsoleFullAccess

`AWSStepFunctionsConsoleFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan akses untuk menyediakan akses pengguna/peran/dll keAWS StepFunctions konsol. Untuk pengalaman

konsol penuh, selain kebijakan ini, pengguna mungkin memerlukanPassRole izin iam: pada peran IAM lain yang dapat diasumsikan oleh layanan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSStepFunctionsConsoleFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Januari 2017, 21:54 UTC
- Waktu yang telah diedit: 12 Januari 2017 09.19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/StatesExecutionRole*"
    },
    {
      "Effect" : "Allow",
      "Action" : "lambda:ListFunctions",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSStepFunctionsFullAccess

`AWSStepFunctionsFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan akses untuk menyediakan akses pengguna/peran/dll keAWS StepFunctions API. Untuk akses penuh, selain kebijakan ini, pengguna HARUS memilikiPassRole izin iam: pada setidaknya satu peran IAM yang dapat diasumsikan oleh layanan.

Menggunakan kebijakan

Anda dapat melampirkan`AWSStepFunctionsFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Januari 2017, 21:51 UTC
- Waktu yang telah diedit: 11 Januari 2017 21.51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas izin identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSStepFunctionsReadOnlyAccess

`AWSStepFunctionsReadOnlyAccess`adalah kebijakanAWS terkelola yang: Kebijakan akses untuk menyediakan akses hanya baca pengguna/peran/dll keAWS StepFunctions layanan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSStepFunctionsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Januari 2017, 21:46 UTC
- Waktu yang telah diedit: 10 November 2017 02.03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:ListActivities",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineForExecution",
        "states:ListExecutions",
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:DescribeActivity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSStorageGatewayFullAccess

`AWSStorageGatewayFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS Storage Gateway melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSStorageGatewayFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 06 September 2022, 20.26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:*"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "fetchStorageGatewayParams",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/storagegateway/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSStorageGatewayReadOnlyAccess

`AWSStorageGatewayReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses keAWS Storage Gateway melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSStorageGatewayReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 06 September 2022, 20.24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:List*",
        "storagegateway:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "fetchStorageGatewayParams",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/storagegateway/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSStorageGatewayServiceRolePolicy

`AWSStorageGatewayServiceRolePolicy`adalah kebijakanAWS terkelola yang: Peran terkait layanan yang digunakan olehAWS Storage Gateway untuk mengaktifkan integrasiAWS layanan lain dengan Storage Gateway.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 Februari 2021, 19:03 UTC
- Waktu yang telah diedit: 17 Februari 2021 09.03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan kebijakan kebijakan kebijakan yang mengizinkan untuk kebijakan terkelara. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSSupplyChainFederationAdminAccess

`AWSSupplyChainFederationAdminAccess`adalah kebijakan AWS terkelola yang: AWSSupplyChainFederationAdminAccess menyediakan akses pengguna federasi Rantai AWS Pasokan ke aplikasi Rantai AWS Pasokan, termasuk izin yang diperlukan untuk melakukan tindakan dalam aplikasi Rantai AWS Pasokan. Kebijakan ini memberikan izin administratif atas pengguna dan grup IAM Identity Center dan dilampirkan ke peran yang dibuat oleh AWS Supply Chain atas nama Anda. Anda tidak boleh melampirkan AWSSupplyChainFederationAdminAccess kebijakan ke entitas IAM lainnya.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSSupplyChainFederationAdminAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Maret 2023, 18:54 UTC

- Waktu telah diedit: 01 November 2023, 18:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSupplyChain",
      "Effect" : "Allow",
      "Action" : [
        "scn:*"
      ],
      "Resource" : [
        "arn:aws:scn:*:*:instance/*"
      ]
    },
    {
      "Sid" : "ChimeAppInstance",
      "Effect" : "Allow",
      "Action" : [
        "chime:BatchCreateChannelMembership",
        "chime:CreateAppInstanceUser",
        "chime:CreateChannel",
        "chime:CreateChannelMembership",
        "chime:CreateChannelModerator",
        "chime:Connect",
        "chime:DeleteChannelMembership",
        "chime:DeleteChannelModerator",
        "chime:DescribeChannelMembershipForAppInstanceUser",
        "chime:GetChannelMembershipPreferences",
```

```
        "chime:ListChannelMemberships",
        "chime:ListChannelMembershipsForAppInstanceUser",
        "chime:ListChannelMessages",
        "chime:ListChannelModerators",
        "chime:TagResource",
        "chime:PutChannelMembershipPreferences",
        "chime:SendChannelMessage",
        "chime:UpdateChannelReadMarker",
        "chime:UpdateAppInstanceUser"
      ],
      "Resource" : [
        "arn:aws:chime:*:*:app-instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SCNInstanceId" : "*"
        }
      }
    },
    {
      "Sid" : "ChimeChannel",
      "Effect" : "Allow",
      "Action" : [
        "chime:DescribeChannel"
      ],
      "Resource" : [
        "arn:aws:chime:*:*:app-instance/*"
      ]
    },
    {
      "Sid" : "ChimeMessaging",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetMessagingSessionEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso:ListDirectoryAssociations",
        "sso:AssociateProfile",
```

```
        "sso:DisassociateProfile",
        "sso:ListProfiles",
        "sso:GetProfile",
        "sso:ListProfileAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AppflowConnectorProfile",
      "Effect" : "Allow",
      "Action" : [
        "appflow:CreateConnectorProfile",
        "appflow:UseConnectorProfile",
        "appflow:DeleteConnectorProfile",
        "appflow:UpdateConnectorProfile"
      ],
      "Resource" : [
        "arn:aws:appflow:*:*:connectorprofile/scn-*"
      ]
    },
    {
      "Sid" : "AppflowFlow",
      "Effect" : "Allow",
      "Action" : [
        "appflow:CreateFlow",
        "appflow:DeleteFlow",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:ListFlows",
        "appflow:StartFlow",
        "appflow:StopFlow",
        "appflow:UpdateFlow",
        "appflow:TagResource",
        "appflow:UntagResource"
      ],
      "Resource" : [
        "arn:aws:appflow:*:*:flow/scn-*"
      ]
    },
    {
      "Sid" : "S3ListAllBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ListSupplyChainBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-supply-chain-data-*"
      ]
    },
    {
      "Sid" : "S3ReadWriteObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-supply-chain-data-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "appflow!*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "SecretsManagerPutResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        },
        "StringEqualsIgnoreCase" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appflow"
        }
      }
    },
    {
      "Sid" : "KMSListKeys",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSListGrants",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListGrants"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceTag/aws-supply-chain-access" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "KMSCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringEquals" : {
          "aws:ResourceTag/aws-supply-chain-access" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSupportAccess

`AWSSupportAccess`adalah kebijakanAWS terkelola yang: Memungkinkan pengguna mengaksesAWS Support Pusat.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSSupportAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 18.41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSSupportAppFullAccess

`AWSSupportAppFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS Support Aplikasi dan layanan lain yang diperlukan, sepertiAWS Support dan Service Quotas. Kebijakan ini mencakup izin untuk menggunakan layanan pendukung sehingga pengguna dapat menghubungiAWS Support kasus dukungan, mengubah kuota layanan, dan membuat peran terkait layanan yang relevan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSSupportAppFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 22 Agustus 2022, 16:53 UTC
- Waktu yang telah diedit: 22 Agustus 2022 16.53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
```

```
        "servicequotas:RequestServiceQuotaIncrease",
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:DescribeSeverityLevels",
        "support:InitiateChatForCase",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSSupportAppReadOnlyAccess

`AWSSupportAppReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca keAWS Support Aplikasi.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSSupportAppReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 22 Agustus 2022, 17:01 UTC
- Waktu yang telah diedit: 22 Agustus 2022, 17.01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeCases",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSSupportPlansFullAccess

`AWSSupportPlansFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke supportplans.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSSupportPlansFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 September 2022, 18:19 UTC
- Waktu yang telah diedit: 09 Mei 2023, 21.07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSSupportPlansReadOnlyAccess

`AWSSupportPlansReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke supportplans.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSSupportPlansReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 September 2022, 18:08 UTC
- Waktu yang telah diedit: 27 September 2022 18.08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSSupportServiceRolePolicy

`AWSSupportServiceRolePolicy`adalah kebijakan AWS terkelola yang: Memungkinkan AWS Support untuk mengakses AWS sumber daya untuk menyediakan layanan penagihan, administrasi, dan dukungan.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 April 2018, 18:04 UTC
- Waktu telah diedit: 17 Januari 2024, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v34 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Statement" : [
    {
      "Sid" : "AWSSupportAPIGatewayAccess",
      "Action" : [
        "apigateway:GET"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
```

```
        "arn:aws:apigateway:*::/domainnames/*/apimappings/*",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models/*/default_template",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "AWSSupportDeleteRoleAccess",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/support.amazonaws.com/
AWSServiceRoleForSupport"
      ]
    },
    {
      "Sid" : "AWSSupportActions",
      "Action" : [
        "access-analyzer:getAccessPreview",
        "access-analyzer:getAnalyzedResource",
```

```
        "access-analyzer:getAnalyzer",
        "access-analyzer:getArchiveRule",
        "access-analyzer:getFinding",
        "access-analyzer:getGeneratedPolicy",
        "access-analyzer:listAccessPreviewFindings",
        "access-analyzer:listAccessPreviews",
        "access-analyzer:listAnalyzedResources",
        "access-analyzer:listAnalyzers",
        "access-analyzer:listArchiveRules",
        "access-analyzer:listFindings",
        "access-analyzer:listPolicyGenerations",
        "acm-pca:describeCertificateAuthority",
        "acm-pca:describeCertificateAuthorityAuditReport",
        "acm-pca:getCertificate",
        "acm-pca:getCertificateAuthorityCertificate",
        "acm-pca:getCertificateAuthorityCsr",
        "acm-pca:listCertificateAuthorities",
        "acm-pca:listTags",
        "acm:describeCertificate",
        "acm:getAccountConfiguration",
        "acm:getCertificate",
        "acm:listCertificates",
        "acm:listTagsForCertificate",
        "airflow:getEnvironment",
        "airflow:listEnvironments",
        "airflow:listTagsForResource",
        "amplify:getApp",
        "amplify:getBackendEnvironment",
        "amplify:getBranch",
        "amplify:getDomainAssociation",
        "amplify:getJob",
        "amplify:getWebhook",
        "amplify:listApps",
        "amplify:listBackendEnvironments",
        "amplify:listBranches",
        "amplify:listDomainAssociations",
        "amplify:listWebhooks",
        "amplifyuibuilder:exportComponents",
        "amplifyuibuilder:exportThemes",
        "appflow:describeConnectorEntity",
        "appflow:describeConnectorProfiles",
        "appflow:describeConnectors",
        "appflow:describeFlow",
        "appflow:describeFlowExecutionRecords",
```

```
        "appflow:listConnectorEntities",
        "appflow:listFlows",
        "application-autoscaling:describeScalableTargets",
        "application-autoscaling:describeScalingActivities",
        "application-autoscaling:describeScalingPolicies",
        "application-autoscaling:describeScheduledActions",
        "applicationinsights:describeApplication",
        "applicationinsights:describeComponent",
        "applicationinsights:describeComponentConfiguration",
        "applicationinsights:describeComponentConfigurationRecommendation",
        "applicationinsights:describeLogPattern",
        "applicationinsights:describeObservation",
        "applicationinsights:describeProblem",
        "applicationinsights:describeProblemObservations",
        "applicationinsights:listApplications",
        "applicationinsights:listComponents",
        "applicationinsights:listConfigurationHistory",
        "applicationinsights:listLogPatterns",
        "applicationinsights:listLogPatternSets",
        "applicationinsights:listProblems",
        "appmesh:describeGatewayRoute",
        "appmesh:describeMesh",
        "appmesh:describeRoute",
        "appmesh:describeVirtualGateway",
        "appmesh:describeVirtualNode",
        "appmesh:describeVirtualRouter",
        "appmesh:describeVirtualService",
        "appmesh:listGatewayRoutes",
        "appmesh:listMeshes",
        "appmesh:listRoutes",
        "appmesh:listTagsForResource",
        "appmesh:listVirtualGateways",
        "appmesh:listVirtualNodes",
        "appmesh:listVirtualRouters",
        "appmesh:listVirtualServices",
        "apprunner:describeAutoScalingConfiguration",
        "apprunner:describeCustomDomains",
        "apprunner:describeOperation",
        "apprunner:describeService",
        "apprunner:listAutoScalingConfigurations",
        "apprunner:listConnections",
        "apprunner:listOperations",
        "apprunner:listServices",
        "apprunner:listTagsForResource",
```

```
        "appstream:describeAppBlockBuilderAppBlockAssociations",
        "appstream:describeAppBlockBuilders",
        "appstream:describeAppBlocks",
        "appstream:describeApplicationFleetAssociations",
        "appstream:describeApplications",
        "appstream:describeDirectoryConfigs",
        "appstream:describeEntitlements",
        "appstream:describeFleets",
        "appstream:describeImageBuilders",
        "appstream:describeImagePermissions",
        "appstream:describeImages",
        "appstream:describeSessions",
        "appstream:describeStacks",
        "appstream:describeUsageReportSubscriptions",
        "appstream:describeUsers",
        "appstream:describeUserStackAssociations",
        "appstream:listAssociatedFleets",
        "appstream:listAssociatedStacks",
        "appstream:listEntitledApplications",
        "appstream:listTagsForResource",
        "appsync:getApiAssociation",
        "appsync:getApiCache",
        "appsync:getDomainName",
        "appsync:getFunction",
        "appsync:getGraphqlApi",
        "appsync:getIntrospectionSchema",
        "appsync:getResolver",
        "appsync:getSchemaCreationStatus",
        "appsync:getSourceApiAssociation",
        "appsync:getType",
        "appsync:listDataSources",
        "appsync:listDomainNames",
        "appsync:listFunctions",
        "appsync:listGraphqlApis",
        "appsync:listResolvers",
        "appsync:listResolversByFunction",
        "appsync:listSourceApiAssociations",
        "appsync:listTypes",
        "appsync:listTypesByAssociation",
        "aps:describeAlertManagerDefinition",
        "aps:describeRuleGroupsNamespace",
        "aps:describeWorkspace",
        "aps:listRuleGroupsNamespaces",
        "aps:listWorkspaces",
```

```
        "athena:batchGetNamedQuery",
        "athena:batchGetQueryExecution",
        "athena:getCalculationExecution",
        "athena:getCalculationExecutionStatus",
        "athena:getDataCatalog",
        "athena:getNamedQuery",
        "athena:getNotebookMetadata",
        "athena:getQueryExecution",
        "athena:getQueryRuntimeStatistics",
        "athena:getSession",
        "athena:getSessionStatus",
        "athena:getWorkGroup",
        "athena:listApplicationDPUSizes",
        "athena:listCalculationExecutions",
        "athena:listDataCatalogs",
        "athena:listEngineVersions",
        "athena:listExecutors",
        "athena:listNamedQueries",
        "athena:listNotebookMetadata",
        "athena:listNotebookSessions",
        "athena:listQueryExecutions",
        "athena:listSessions",
        "athena:listTagsForResource",
        "athena:listWorkGroups",
        "auditmanager:getAccountStatus",
        "auditmanager:getDelegations",
        "auditmanager:listAssessmentFrameworks",
        "auditmanager:listAssessmentReports",
        "auditmanager:listAssessments",
        "auditmanager:listControls",
        "auditmanager:listKeywordsForDataSource",
        "auditmanager:listNotifications",
        "autoscaling-plans:describeScalingPlanResources",
        "autoscaling-plans:describeScalingPlans",
        "autoscaling-plans:getScalingPlanResourceForecastData",
        "autoscaling:describeAccountLimits",
        "autoscaling:describeAdjustmentTypes",
        "autoscaling:describeAutoScalingGroups",
        "autoscaling:describeAutoScalingInstances",
        "autoscaling:describeAutoScalingNotificationTypes",
        "autoscaling:describeInstanceRefreshes",
        "autoscaling:describeLaunchConfigurations",
        "autoscaling:describeLifecycleHooks",
        "autoscaling:describeLifecycleHookTypes",
```

```
        "autoscaling:describeLoadBalancers",
        "autoscaling:describeLoadBalancerTargetGroups",
        "autoscaling:describeMetricCollectionTypes",
        "autoscaling:describeNotificationConfigurations",
        "autoscaling:describePolicies",
        "autoscaling:describeScalingActivities",
        "autoscaling:describeScalingProcessTypes",
        "autoscaling:describeScheduledActions",
        "autoscaling:describeTags",
        "autoscaling:describeTerminationPolicyTypes",
        "autoscaling:describeWarmPool",
        "backup:describeBackupJob",
        "backup:describeBackupVault",
        "backup:describeCopyJob",
        "backup:describeFramework",
        "backup:describeGlobalSettings",
        "backup:describeProtectedResource",
        "backup:describeRecoveryPoint",
        "backup:describeRegionSettings",
        "backup:describeReportJob",
        "backup:describeReportPlan",
        "backup:describeRestoreJob",
        "backup:getBackupPlan",
        "backup:getBackupPlanFromJSON",
        "backup:getBackupPlanFromTemplate",
        "backup:getBackupSelection",
        "backup:getBackupVaultAccessPolicy",
        "backup:getBackupVaultNotifications",
        "backup:getLegalHold",
        "backup:getRecoveryPointRestoreMetadata",
        "backup:getSupportedResourceTypes",
        "backup:listBackupJobs",
        "backup:listBackupPlans",
        "backup:listBackupPlanTemplates",
        "backup:listBackupPlanVersions",
        "backup:listBackupSelections",
        "backup:listBackupVaults",
        "backup:listCopyJobs",
        "backup:listFrameworks",
        "backup:listLegalHolds",
        "backup:listProtectedResources",
        "backup:listRecoveryPointsByBackupVault",
        "backup:listRecoveryPointsByLegalHold",
        "backup:listRecoveryPointsByResource",
```

```
        "backup:listReportJobs",
        "backup:listReportPlans",
        "backup:listRestoreJobs",
        "backup:listTags",
        "backup-gateway:getGateway",
        "backup-gateway:getHypervisor",
        "backup-gateway:getHypervisorPropertyMappings",
        "backup-gateway:getVirtualMachine",
        "backup-gateway:listGateways",
        "backup-gateway:listHypervisors",
        "backup-gateway:listVirtualMachines",
        "batch:describeComputeEnvironments",
        "batch:describeJobDefinitions",
        "batch:describeJobQueues",
        "batch:describeJobs",
        "batch:listJobs",
        "braket:getDevice",
        "braket:getQuantumTask",
        "braket:searchDevices",
        "braket:searchQuantumTasks",
        "budgets:viewBudget",
        "ce:getCostAndUsage",
        "ce:getCostAndUsageWithResources",
        "ce:getCostForecast",
        "ce:getDimensionValues",
        "ce:getReservationCoverage",
        "ce:getReservationPurchaseRecommendation",
        "ce:getReservationUtilization",
        "ce:getRightsizingRecommendation",
        "ce:getSavingsPlansCoverage",
        "ce:getSavingsPlansPurchaseRecommendation",
        "ce:getSavingsPlansUtilization",
        "ce:getSavingsPlansUtilizationDetails",
        "ce:getTags",
        "chime:describeAppInstance",
        "chime:getAttendee",
        "chime:getGlobalSettings",
        "chime:getMediaCapturePipeline",
        "chime:getMediaPipeline",
        "chime:getMeeting",
        "chime:getProxySession",
        "chime:getSipMediaApplication",
        "chime:getSipRule",
        "chime:getVoiceConnector",
```

```
        "chime:getVoiceConnectorGroup",
        "chime:getVoiceConnectorLoggingConfiguration",
        "chime:listAppInstances",
        "chime:listAttendees",
        "chime:listChannelBans",
        "chime:listChannels",
        "chime:listChannelsModeratedByAppInstanceUser",
        "chime:listMediaCapturePipelines",
        "chime:listMediaPipelines",
        "chime:listMeetings",
        "chime:listSipMediaApplications",
        "chime:listSipRules",
        "chime:listVoiceConnectorGroups",
        "chime:listVoiceConnectors",
        "cleanrooms:batchGetCollaborationAnalysisTemplate",
        "cleanrooms:batchGetSchema",
        "cleanrooms:getAnalysisTemplate",
        "cleanrooms:getCollaboration",
        "cleanrooms:getCollaborationAnalysisTemplate",
        "cleanrooms:getConfiguredTable",
        "cleanrooms:getConfiguredTableAssociation",
        "cleanrooms:getMembership",
        "cleanrooms:getSchema",
        "cleanrooms:listAnalysisTemplates",
        "cleanrooms:listCollaborationAnalysisTemplates",
        "cleanrooms:listCollaborations",
        "cleanrooms:listConfiguredTableAssociations",
        "cleanrooms:listConfiguredTables",
        "cleanrooms:listMembers",
        "cleanrooms:listMemberships",
        "cleanrooms:listSchemas",
        "cloud9:describeEnvironmentMemberships",
        "cloud9:describeEnvironments",
        "cloud9:listEnvironments",
        "clouddirectory:getDirectory",
        "clouddirectory:listDirectories",
        "cloudformation:batchDescribeTypeConfigurations",
        "cloudformation:describeAccountLimits",
        "cloudformation:describeChangeSet",
        "cloudformation:describeChangeSetHooks",
        "cloudformation:describePublisher",
        "cloudformation:describeStackEvents",
        "cloudformation:describeStackInstance",
        "cloudformation:describeStackResource",
```

```
        "cloudformation:describeStackResources",
        "cloudformation:describeStacks",
        "cloudformation:describeStackSet",
        "cloudformation:describeStackSetOperation",
        "cloudformation:describeType",
        "cloudformation:describeTypeRegistration",
        "cloudformation:estimateTemplateCost",
        "cloudformation:getStackPolicy",
        "cloudformation:getTemplate",
        "cloudformation:getTemplateSummary",
        "cloudformation:listChangeSets",
        "cloudformation:listExports",
        "cloudformation:listImports",
        "cloudformation:listStackInstances",
        "cloudformation:listStackResources",
        "cloudformation:listStacks",
        "cloudformation:listStackSetOperationResults",
        "cloudformation:listStackSetOperations",
        "cloudformation:listStackSets",
        "cloudformation:listTypeRegistrations",
        "cloudformation:listTypes",
        "cloudformation:listTypeVersions",
        "cloudfront:describeFunction",
        "cloudfront:getCachePolicy",
        "cloudfront:getCachePolicyConfig",
        "cloudfront:getCloudFrontOriginAccessIdentity",
        "cloudfront:getCloudFrontOriginAccessIdentityConfig",
        "cloudfront:getContinuousDeploymentPolicy",
        "cloudfront:getContinuousDeploymentPolicyConfig",
        "cloudfront:getDistribution",
        "cloudfront:getDistributionConfig",
        "cloudfront:getInvalidation",
        "cloudfront:getKeyGroup",
        "cloudfront:getKeyGroupConfig",
        "cloudfront:getMonitoringSubscription",
        "cloudfront:getOriginAccessControl",
        "cloudfront:getOriginAccessControlConfig",
        "cloudfront:getOriginRequestPolicy",
        "cloudfront:getOriginRequestPolicyConfig",
        "cloudfront:getPublicKey",
        "cloudfront:getPublicKeyConfig",
        "cloudfront:getRealtimeLogConfig",
        "cloudfront:getStreamingDistribution",
        "cloudfront:getStreamingDistributionConfig",
```

```
        "cloudfront:listCachePolicies",
        "cloudfront:listCloudFrontOriginAccessIdentities",
        "cloudfront:listContinuousDeploymentPolicies",
        "cloudfront:listDistributions",
        "cloudfront:listDistributionsByCachePolicyId",
        "cloudfront:listDistributionsByKeyGroup",
        "cloudfront:listDistributionsByOriginRequestPolicyId",
        "cloudfront:listDistributionsByRealtimeLogConfig",
        "cloudfront:listDistributionsByResponseHeadersPolicyId",
        "cloudfront:listDistributionsByWebACLId",
        "cloudfront:listFunctions",
        "cloudfront:listInvalidations",
        "cloudfront:listKeyGroups",
        "cloudfront:listOriginAccessControls",
        "cloudfront:listOriginRequestPolicies",
        "cloudfront:listPublicKeys",
        "cloudfront:listRealtimeLogConfigs",
        "cloudfront:listStreamingDistributions",
        "cloudhsm:describeBackups",
        "cloudhsm:describeClusters",
        "cloudsearch:describeAnalysisSchemes",
        "cloudsearch:describeAvailabilityOptions",
        "cloudsearch:describeDomains",
        "cloudsearch:describeExpressions",
        "cloudsearch:describeIndexFields",
        "cloudsearch:describeScalingParameters",
        "cloudsearch:describeServiceAccessPolicies",
        "cloudsearch:describeSuggesters",
        "cloudsearch:listDomainNames",
        "cloudtrail:describeTrails",
        "cloudtrail:getEventSelectors",
        "cloudtrail:getInsightSelectors",
        "cloudtrail:getTrail",
        "cloudtrail:getTrailStatus",
        "cloudtrail:listPublicKeys",
        "cloudtrail:listTags",
        "cloudtrail:listTrails",
        "cloudtrail:lookupEvents",
        "cloudwatch:describeAlarmHistory",
        "cloudwatch:describeAlarms",
        "cloudwatch:describeAlarmsForMetric",
        "cloudwatch:describeAnomalyDetectors",
        "cloudwatch:describeInsightRules",
        "cloudwatch:getDashboard",
```

```
        "cloudwatch:getInsightRuleReport",
        "cloudwatch:getMetricData",
        "cloudwatch:getMetricStatistics",
        "cloudwatch:getMetricStream",
        "cloudwatch:listDashboards",
        "cloudwatch:listManagedInsightRules",
        "cloudwatch:listMetrics",
        "cloudwatch:listMetricStreams",
        "codeartifact:describeDomain",
        "codeartifact:describePackageVersion",
        "codeartifact:describeRepository",
        "codeartifact:getDomainPermissionsPolicy",
        "codeartifact:getRepositoryEndpoint",
        "codeartifact:getRepositoryPermissionsPolicy",
        "codeartifact:listDomains",
        "codeartifact:listPackages",
        "codeartifact:listPackageVersionAssets",
        "codeartifact:listPackageVersions",
        "codeartifact:listRepositories",
        "codeartifact:listRepositoriesInDomain",
        "codebuild:batchGetBuildBatches",
        "codebuild:batchGetBuilds",
        "codebuild:batchGetProjects",
        "codebuild:listBuildBatches",
        "codebuild:listBuildBatchesForProject",
        "codebuild:listBuilds",
        "codebuild:listBuildsForProject",
        "codebuild:listCuratedEnvironmentImages",
        "codebuild:listProjects",
        "codebuild:listSourceCredentials",
        "codecommit:batchGetRepositories",
        "codecommit:getBranch",
        "codecommit:getRepository",
        "codecommit:getRepositoryTriggers",
        "codecommit:listBranches",
        "codecommit:listRepositories",
        "codedeploy:batchGetApplicationRevisions",
        "codedeploy:batchGetApplications",
        "codedeploy:batchGetDeploymentGroups",
        "codedeploy:batchGetDeploymentInstances",
        "codedeploy:batchGetDeployments",
        "codedeploy:batchGetDeploymentTargets",
        "codedeploy:batchGetOnPremisesInstances",
        "codedeploy:getApplication",
```

```
        "codedeploy:getApplicationRevision",
        "codedeploy:getDeployment",
        "codedeploy:getDeploymentConfig",
        "codedeploy:getDeploymentGroup",
        "codedeploy:getDeploymentInstance",
        "codedeploy:getDeploymentTarget",
        "codedeploy:getOnPremisesInstance",
        "codedeploy:listApplicationRevisions",
        "codedeploy:listApplications",
        "codedeploy:listDeploymentConfigs",
        "codedeploy:listDeploymentGroups",
        "codedeploy:listDeploymentInstances",
        "codedeploy:listDeployments",
        "codedeploy:listDeploymentTargets",
        "codedeploy:listGitHubAccountTokenNames",
        "codedeploy:listOnPremisesInstances",
        "codepipeline:getJobDetails",
        "codepipeline:getPipeline",
        "codepipeline:getPipelineExecution",
        "codepipeline:getPipelineState",
        "codepipeline:listActionExecutions",
        "codepipeline:listActionTypes",
        "codepipeline:listPipelineExecutions",
        "codepipeline:listPipelines",
        "codepipeline:listWebhooks",
        "codestar:describeProject",
        "codestar:listProjects",
        "codestar:listResources",
        "codestar:listTeamMembers",
        "codestar:listUserProfiles",
        "codestar-connections:getConnection",
        "codestar-connections:getHost",
        "codestar-connections:listConnections",
        "codestar-connections:listHosts",
        "cognito-identity:describeIdentityPool",
        "cognito-identity:getIdentityPoolRoles",
        "cognito-identity:listIdentities",
        "cognito-identity:listIdentityPools",
        "cognito-idp:describeIdentityProvider",
        "cognito-idp:describeResourceServer",
        "cognito-idp:describeRiskConfiguration",
        "cognito-idp:describeUserImportJob",
        "cognito-idp:describeUserPool",
        "cognito-idp:describeUserPoolClient",
```

```
        "cognito-idp:describeUserPoolDomain",
        "cognito-idp:getGroup",
        "cognito-idp:getUICustomization",
        "cognito-idp:getUserPoolMfaConfig",
        "cognito-idp:listGroups",
        "cognito-idp:listIdentityProviders",
        "cognito-idp:listResourceServers",
        "cognito-idp:listUserImportJobs",
        "cognito-idp:listUserPoolClients",
        "cognito-idp:listUserPools",
        "cognito-sync:describeDataset",
        "cognito-sync:describeIdentityPoolUsage",
        "cognito-sync:describeIdentityUsage",
        "cognito-sync:getCognitoEvents",
        "cognito-sync:getIdentityPoolConfiguration",
        "cognito-sync:listDatasets",
        "cognito-sync:listIdentityPoolUsage",
        "comprehend:describeDocumentClassificationJob",
        "comprehend:describeDocumentClassifier",
        "comprehend:describeDominantLanguageDetectionJob",
        "comprehend:describeEndpoint",
        "comprehend:describeEntitiesDetectionJob",
        "comprehend:describeEntityRecognizer",
        "comprehend:describeEventsDetectionJob",
        "comprehend:describeFlywheel",
        "comprehend:describeFlywheelIteration",
        "comprehend:describeKeyPhrasesDetectionJob",
        "comprehend:describePiiEntitiesDetectionJob",
        "comprehend:describeSentimentDetectionJob",
        "comprehend:describeTargetedSentimentDetectionJob",
        "comprehend:describeTopicsDetectionJob",
        "comprehend:listDocumentClassificationJobs",
        "comprehend:listDocumentClassifiers",
        "comprehend:listDominantLanguageDetectionJobs",
        "comprehend:listEndpoints",
        "comprehend:listEntitiesDetectionJobs",
        "comprehend:listEntityRecognizers",
        "comprehend:listEventsDetectionJobs",
        "comprehend:listFlywheelIterationHistory",
        "comprehend:listFlywheels",
        "comprehend:listKeyPhrasesDetectionJobs",
        "comprehend:listPiiEntitiesDetectionJobs",
        "comprehend:listSentimentDetectionJobs",
        "comprehend:listTargetedSentimentDetectionJobs",
```

```
        "comprehend:listTopicsDetectionJobs",
        "compute-optimizer:getAutoScalingGroupRecommendations",
        "compute-optimizer:getEBSVolumeRecommendations",
        "compute-optimizer:getEC2InstanceRecommendations",
        "compute-optimizer:getEC2RecommendationProjectedMetrics",
        "compute-optimizer:getECSServiceRecommendations",
        "compute-optimizer:getECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:getEnrollmentStatus",
        "compute-optimizer:getRecommendationSummaries",
        "config:batchGetAggregateResourceConfig",
        "config:batchGetResourceConfig",
        "config:describeAggregateComplianceByConfigRules",
        "config:describeAggregationAuthorizations",
        "config:describeComplianceByConfigRule",
        "config:describeComplianceByResource",
        "config:describeConfigRuleEvaluationStatus",
        "config:describeConfigRules",
        "config:describeConfigurationAggregators",
        "config:describeConfigurationAggregatorSourcesStatus",
        "config:describeConfigurationRecorders",
        "config:describeConfigurationRecorderStatus",
        "config:describeConformancePackCompliance",
        "config:describeConformancePacks",
        "config:describeConformancePackStatus",
        "config:describeDeliveryChannels",
        "config:describeDeliveryChannelStatus",
        "config:describeOrganizationConfigRules",
        "config:describeOrganizationConfigRuleStatuses",
        "config:describeOrganizationConformancePacks",
        "config:describeOrganizationConformancePackStatuses",
        "config:describePendingAggregationRequests",
        "config:describeRemediationConfigurations",
        "config:describeRemediationExceptions",
        "config:describeRemediationExecutionStatus",
        "config:describeRetentionConfigurations",
        "config:getAggregateComplianceDetailsByConfigRule",
        "config:getAggregateConfigRuleComplianceSummary",
        "config:getAggregateDiscoveredResourceCounts",
        "config:getAggregateResourceConfig",
        "config:getComplianceDetailsByConfigRule",
        "config:getComplianceDetailsByResource",
        "config:getComplianceSummaryByConfigRule",
        "config:getComplianceSummaryByResourceType",
        "config:getConformancePackComplianceDetails",
```

```
        "config:getConformancePackComplianceSummary",
        "config:getDiscoveredResourceCounts",
        "config:getOrganizationConfigRuleDetailedStatus",
        "config:getOrganizationConformancePackDetailedStatus",
        "config:getResourceConfigHistory",
        "config:listAggregateDiscoveredResources",
        "config:listDiscoveredResources",
        "config:listTagsForResource",
        "connect:describeContact",
        "connect:describePhoneNumber",
        "connect:describeQuickConnect",
        "connect:describeUser",
        "connect:getCurrentMetricData",
        "connect:getMetricData",
        "connect:listContactEvaluations",
        "connect:listEvaluationForms",
        "connect:listEvaluationFormVersions",
        "connect:listPhoneNumbersV2",
        "connect:listQuickConnects",
        "connect:listRoutingProfiles",
        "connect:listSecurityProfiles",
        "connect:listUsers",
        "connect:listViews",
        "connect:listViewVersions",
        "controltower:describeAccountFactoryConfig",
        "controltower:describeCoreService",
        "controltower:describeGuardrail",
        "controltower:describeGuardrailForTarget",
        "controltower:describeManagedAccount",
        "controltower:describeSingleSignOn",
        "controltower:getAvailableUpdates",
        "controltower:getHomeRegion",
        "controltower:getLandingZoneStatus",
        "controltower:listDirectoryGroups",
        "controltower:listGuardrailsForTarget",
        "controltower:listGuardrailViolations",
        "controltower:listManagedAccounts",
        "controltower:listManagedAccountsForGuardrail",
        "controltower:listManagedAccountsForParent",
        "controltower:listManagedOrganizationalUnits",
        "controltower:listManagedOrganizationalUnitsForGuardrail",
        "databrew:describeDataset",
        "databrew:describeJob",
        "databrew:describeProject",
```

```
        "databrew:describeRecipe",
        "databrew:listDatasets",
        "databrew:listJobRuns",
        "databrew:listJobs",
        "databrew:listProjects",
        "databrew:listRecipes",
        "databrew:listRecipeVersions",
        "databrew:listTagsForResource",
        "datapipeline:describeObjects",
        "datapipeline:describePipelines",
        "datapipeline:getPipelineDefinition",
        "datapipeline:listPipelines",
        "datapipeline:queryObjects",
        "datasync:describeAgent",
        "datasync:describeLocationEfs",
        "datasync:describeLocationFsxLustre",
        "datasync:describeLocationFsxOpenZfs",
        "datasync:describeLocationFsxWindows",
        "datasync:describeLocationHdfs",
        "datasync:describeLocationNfs",
        "datasync:describeLocationObjectStorage",
        "datasync:describeLocationS3",
        "datasync:describeLocationSmb",
        "datasync:describeTask",
        "datasync:describeTaskExecution",
        "datasync:listAgents",
        "datasync:listLocations",
        "datasync:listTaskExecutions",
        "datasync:listTasks",
        "dax:describeClusters",
        "dax:describeDefaultParameters",
        "dax:describeEvents",
        "dax:describeParameterGroups",
        "dax:describeParameters",
        "dax:describeSubnetGroups",
        "detective:getMembers",
        "detective:listGraphs",
        "detective:listInvitations",
        "detective:listMembers",
        "devicefarm:getAccountSettings",
        "devicefarm:getDevice",
        "devicefarm:getDevicePool",
        "devicefarm:getDevicePoolCompatibility",
        "devicefarm:getJob",
```

```
        "devicefarm:getProject",
        "devicefarm:getRemoteAccessSession",
        "devicefarm:getRun",
        "devicefarm:getSuite",
        "devicefarm:getTest",
        "devicefarm:getTestGridProject",
        "devicefarm:getTestGridSession",
        "devicefarm:getUpload",
        "devicefarm:listArtifacts",
        "devicefarm:listDevicePools",
        "devicefarm:listDevices",
        "devicefarm:listJobs",
        "devicefarm:listProjects",
        "devicefarm:listRemoteAccessSessions",
        "devicefarm:listRuns",
        "devicefarm:listSamples",
        "devicefarm:listSuites",
        "devicefarm:listTestGridProjects",
        "devicefarm:listTestGridSessionActions",
        "devicefarm:listTestGridSessionArtifacts",
        "devicefarm:listTestGridSessions",
        "devicefarm:listTests",
        "devicefarm:listUniqueProblems",
        "devicefarm:listUploads",
        "directconnect:describeConnectionLoa",
        "directconnect:describeConnections",
        "directconnect:describeConnectionsOnInterconnect",
        "directconnect:describeCustomerMetadata",
        "directconnect:describeDirectConnectGatewayAssociationProposals",
        "directconnect:describeDirectConnectGatewayAssociations",
        "directconnect:describeDirectConnectGatewayAttachments",
        "directconnect:describeDirectConnectGateways",
        "directconnect:describeHostedConnections",
        "directconnect:describeInterconnectLoa",
        "directconnect:describeInterconnects",
        "directconnect:describeLags",
        "directconnect:describeLoa",
        "directconnect:describeLocations",
        "directconnect:describeRouterConfiguration",
        "directconnect:describeVirtualGateways",
        "directconnect:describeVirtualInterfaces",
        "dlm:getLifecyclePolicies",
        "dlm:getLifecyclePolicy",
        "dms:describeAccountAttributes",
```

```
        "dms:describeApplicableIndividualAssessments",
        "dms:describeConnections",
        "dms:describeEndpoints",
        "dms:describeEndpointSettings",
        "dms:describeEndpointTypes",
        "dms:describeEventCategories",
        "dms:describeEvents",
        "dms:describeEventSubscriptions",
        "dms:describeFleetAdvisorCollectors",
        "dms:describeFleetAdvisorDatabases",
        "dms:describeFleetAdvisorLsaAnalysis",
        "dms:describeFleetAdvisorSchemaObjectSummary",
        "dms:describeFleetAdvisorSchemas",
        "dms:describeOrderableReplicationInstances",
        "dms:describePendingMaintenanceActions",
        "dms:describeRefreshSchemasStatus",
        "dms:describeReplicationInstances",
        "dms:describeReplicationInstanceTaskLogs",
        "dms:describeReplicationSubnetGroups",
        "dms:describeReplicationTaskAssessmentResults",
        "dms:describeReplicationTaskAssessmentRuns",
        "dms:describeReplicationTaskIndividualAssessments",
        "dms:describeReplicationTasks",
        "dms:describeSchemas",
        "dms:describeTableStatistics",
        "docdb-elastic:getCluster",
        "docdb-elastic:getClusterSnapshot",
        "docdb-elastic:listClusters",
        "docdb-elastic:listClusterSnapshots",
        "drs:describeJobLogItems",
        "drs:describeJobs",
        "drs:describeLaunchConfigurationTemplates",
        "drs:describeRecoveryInstances",
        "drs:describeRecoverySnapshots",
        "drs:describeReplicationConfigurationTemplates",
        "drs:describeSourceNetworks",
        "drs:describeSourceServers",
        "drs:getLaunchConfiguration",
        "drs:getReplicationConfiguration",
        "drs:listExtensibleSourceServers",
        "drs:listLaunchActions",
        "drs:listStagingAccounts",
        "ds:describeClientAuthenticationSettings",
        "ds:describeConditionalForwarders",
```

```
        "ds:describeDirectories",
        "ds:describeDomainControllers",
        "ds:describeEventTopics",
        "ds:describeLDAPSSettings",
        "ds:describeSharedDirectories",
        "ds:describeSnapshots",
        "ds:describeTrusts",
        "ds:getDirectoryLimits",
        "ds:getSnapshotLimits",
        "ds:listIpRoutes",
        "ds:listSchemaExtensions",
        "ds:listTagsForResource",
        "dynamodb:describeBackup",
        "dynamodb:describeContinuousBackups",
        "dynamodb:describeContributorInsights",
        "dynamodb:describeExport",
        "dynamodb:describeGlobalTable",
        "dynamodb:describeImport",
        "dynamodb:describeKinesisStreamingDestination",
        "dynamodb:describeLimits",
        "dynamodb:describeStream",
        "dynamodb:describeTable",
        "dynamodb:describeTimeToLive",
        "dynamodb:listBackups",
        "dynamodb:listContributorInsights",
        "dynamodb:listExports",
        "dynamodb:listGlobalTables",
        "dynamodb:listImports",
        "dynamodb:listStreams",
        "dynamodb:listTables",
        "dynamodb:listTagsOfResource",
        "ec2:describeAccountAttributes",
        "ec2:describeAddresses",
        "ec2:describeAddressesAttribute",
        "ec2:describeAddressTransfers",
        "ec2:describeAggregateIdFormat",
        "ec2:describeAvailabilityZones",
        "ec2:describeBundleTasks",
        "ec2:describeByoipCidrs",
        "ec2:describeCapacityReservationFleets",
        "ec2:describeCapacityReservations",
        "ec2:describeCarrierGateways",
        "ec2:describeClassicLinkInstances",
        "ec2:describeClientVpnAuthorizationRules",
```

```
        "ec2:describeClientVpnConnections",
        "ec2:describeClientVpnEndpoints",
        "ec2:describeClientVpnRoutes",
        "ec2:describeClientVpnTargetNetworks",
        "ec2:describeCoipPools",
        "ec2:describeConversionTasks",
        "ec2:describeCustomerGateways",
        "ec2:describeDhcpOptions",
        "ec2:describeEgressOnlyInternetGateways",
        "ec2:describeExportImageTasks",
        "ec2:describeExportTasks",
        "ec2:describeFastLaunchImages",
        "ec2:describeFastSnapshotRestores",
        "ec2:describeFleetHistory",
        "ec2:describeFleetInstances",
        "ec2:describeFleets",
        "ec2:describeFlowLogs",
        "ec2:describeFpgaImageAttribute",
        "ec2:describeFpgaImages",
        "ec2:describeHostReservationOfferings",
        "ec2:describeHostReservations",
        "ec2:describeHosts",
        "ec2:describeIamInstanceProfileAssociations",
        "ec2:describeIdentityIdFormat",
        "ec2:describeIdFormat",
        "ec2:describeImageAttribute",
        "ec2:describeImages",
        "ec2:describeImportImageTasks",
        "ec2:describeImportSnapshotTasks",
        "ec2:describeInstanceAttribute",
        "ec2:describeInstanceCreditSpecifications",
        "ec2:describeInstanceEventNotificationAttributes",
        "ec2:describeInstanceEventWindows",
        "ec2:describeInstances",
        "ec2:describeInstanceStatus",
        "ec2:describeInstanceTypeOfferings",
        "ec2:describeInstanceTypes",
        "ec2:describeInternetGateways",
        "ec2:describeIpamPools",
        "ec2:describeIpams",
        "ec2:describeIpamScopes",
        "ec2:describeIpv6Pools",
        "ec2:describeKeyPairs",
        "ec2:describeLaunchTemplates",
```

```
        "ec2:describeLaunchTemplateVersions",
        "ec2:describeLocalGatewayRouteTables",
        "ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:describeLocalGatewayRouteTableVpcAssociations",
        "ec2:describeLocalGateways",
        "ec2:describeLocalGatewayVirtualInterfaceGroups",
        "ec2:describeLocalGatewayVirtualInterfaces",
        "ec2:describeManagedPrefixLists",
        "ec2:describeMovingAddresses",
        "ec2:describeNatGateways",
        "ec2:describeNetworkAcls",
        "ec2:describeNetworkInterfaceAttribute",
        "ec2:describeNetworkInterfaces",
        "ec2:describePlacementGroups",
        "ec2:describePrefixLists",
        "ec2:describePrincipalIdFormat",
        "ec2:describePublicIpv4Pools",
        "ec2:describeRegions",
        "ec2:describeReservedInstances",
        "ec2:describeReservedInstancesListings",
        "ec2:describeReservedInstancesModifications",
        "ec2:describeReservedInstancesOfferings",
        "ec2:describeRouteTables",
        "ec2:describeScheduledInstanceAvailability",
        "ec2:describeScheduledInstances",
        "ec2:describeSecurityGroupReferences",
        "ec2:describeSecurityGroupRules",
        "ec2:describeSecurityGroups",
        "ec2:describeSnapshotAttribute",
        "ec2:describeSnapshots",
        "ec2:describeSpotDatafeedSubscription",
        "ec2:describeSpotFleetInstances",
        "ec2:describeSpotFleetRequestHistory",
        "ec2:describeSpotFleetRequests",
        "ec2:describeSpotInstanceRequests",
        "ec2:describeSpotPriceHistory",
        "ec2:describeStaleSecurityGroups",
        "ec2:describeStoreImageTasks",
        "ec2:describeSubnets",
        "ec2:describeTags",
        "ec2:describeTrafficMirrorFilters",
        "ec2:describeTrafficMirrorSessions",
        "ec2:describeTrafficMirrorTargets",
        "ec2:describeTransitGatewayAttachments",
```

```
        "ec2:describeTransitGatewayConnectPeers",
        "ec2:describeTransitGatewayMulticastDomains",
        "ec2:describeTransitGatewayPeeringAttachments",
        "ec2:describeTransitGatewayPolicyTables",
        "ec2:describeTransitGatewayRouteTableAnnouncements",
        "ec2:describeTransitGatewayRouteTables",
        "ec2:describeTransitGateways",
        "ec2:describeTransitGatewayVpcAttachments",
        "ec2:describeVerifiedAccessEndpoints",
        "ec2:describeVerifiedAccessGroups",
        "ec2:describeVerifiedAccessInstances",
        "ec2:describeVerifiedAccessTrustProviders",
        "ec2:describeVolumeAttribute",
        "ec2:describeVolumes",
        "ec2:describeVolumesModifications",
        "ec2:describeVolumeStatus",
        "ec2:describeVpcAttribute",
        "ec2:describeVpcClassicLink",
        "ec2:describeVpcClassicLinkDnsSupport",
        "ec2:describeVpcEndpointConnectionNotifications",
        "ec2:describeVpcEndpointConnections",
        "ec2:describeVpcEndpoints",
        "ec2:describeVpcEndpointServiceConfigurations",
        "ec2:describeVpcEndpointServicePermissions",
        "ec2:describeVpcEndpointServices",
        "ec2:describeVpcPeeringConnections",
        "ec2:describeVpcs",
        "ec2:describeVpnConnections",
        "ec2:describeVpnGateways",
        "ec2:getAssociatedIpv6PoolCidrs",
        "ec2:getCapacityReservationUsage",
        "ec2:getCoipPoolUsage",
        "ec2:getConsoleOutput",
        "ec2:getConsoleScreenshot",
        "ec2:getDefaultCreditSpecification",
        "ec2:getEbsDefaultKmsKeyId",
        "ec2:getEbsEncryptionByDefault",
        "ec2:getGroupsForCapacityReservation",
        "ec2:getHostReservationPurchasePreview",
        "ec2:getInstanceTypesFromInstanceRequirements",
        "ec2:getIpamAddressHistory",
        "ec2:getIpamPoolAllocations",
        "ec2:getIpamPoolCidrs",
        "ec2:getIpamResourceCidrs",
```

```
        "ec2:getLaunchTemplateData",
        "ec2:getManagedPrefixListAssociations",
        "ec2:getManagedPrefixListEntries",
        "ec2:getReservedInstancesExchangeQuote",
        "ec2:getSerialConsoleAccessStatus",
        "ec2:getSpotPlacementScores",
        "ec2:getTransitGatewayMulticastDomainAssociations",
        "ec2:getTransitGatewayPrefixListReferences",
        "ec2:getVerifiedAccessEndpointPolicy",
        "ec2:getVerifiedAccessGroupPolicy",
        "ec2:listImagesInRecycleBin",
        "ec2:listSnapshotsInRecycleBin",
        "ec2:searchLocalGatewayRoutes",
        "ec2:searchTransitGatewayMulticastGroups",
        "ec2:searchTransitGatewayRoutes",
        "ecr-public:describeImages",
        "ecr-public:describeImageTags",
        "ecr-public:describeRegistries",
        "ecr-public:describeRepositories",
        "ecr-public:getRegistryCatalogData",
        "ecr-public:getRepositoryCatalogData",
        "ecr-public:getRepositoryPolicy",
        "ecr-public:listTagsForResource",
        "ecr:batchCheckLayerAvailability",
        "ecr:batchGetRepositoryScanningConfiguration",
        "ecr:describeImages",
        "ecr:describeImageReplicationStatus",
        "ecr:describeImageScanFindings",
        "ecr:describePullThroughCacheRules",
        "ecr:describeRegistry",
        "ecr:describeRepositories",
        "ecr:getLifecyclePolicy",
        "ecr:getLifecyclePolicyPreview",
        "ecr:getRegistryPolicy",
        "ecr:getRegistryScanningConfiguration",
        "ecr:getRepositoryPolicy",
        "ecr:listImages",
        "ecr:listTagsForResource",
        "ecs:describeCapacityProviders",
        "ecs:describeClusters",
        "ecs:describeContainerInstances",
        "ecs:describeServices",
        "ecs:describeTaskDefinition",
        "ecs:describeTasks",
```

```
        "ecs:describeTaskSets",
        "ecs:getTaskProtection",
        "ecs:listAccountSettings",
        "ecs:listAttributes",
        "ecs:listClusters",
        "ecs:listContainerInstances",
        "ecs:listServices",
        "ecs:listServicesByNamespace",
        "ecs:listTagsForResource",
        "ecs:listTaskDefinitionFamilies",
        "ecs:listTaskDefinitions",
        "ecs:listTasks",
        "eks:describeAccessEntry",
        "eks:describeAddon",
        "eks:describeAddonConfiguration",
        "eks:describeAddonVersions",
        "eks:describeCluster",
        "eks:describeEksAnywhereSubscription",
        "eks:describeFargateProfile",
        "eks:describeIdentityProviderConfig",
        "eks:describeNodegroup",
        "eks:describeUpdate",
        "eks:listAccessEntries",
        "eks:listAccessPolicies",
        "eks:listAddons",
        "eks:listAssociatedAccessPolicies",
        "eks:listClusters",
        "eks:listEksAnywhereSubscriptions",
        "eks:listFargateProfiles",
        "eks:listIdentityProviderConfigs",
        "eks:listNodegroups",
        "eks:listUpdates",
        "elasticache:describeCacheClusters",
        "elasticache:describeCacheEngineVersions",
        "elasticache:describeCacheParameterGroups",
        "elasticache:describeCacheParameters",
        "elasticache:describeCacheSecurityGroups",
        "elasticache:describeCacheSubnetGroups",
        "elasticache:describeEngineDefaultParameters",
        "elasticache:describeEvents",
        "elasticache:describeGlobalReplicationGroups",
        "elasticache:describeReplicationGroups",
        "elasticache:describeReservedCacheNodes",
        "elasticache:describeReservedCacheNodesOfferings",
```

```
        "elasticache:describeServerlessCaches",
        "elasticache:describeServerlessCacheSnapshots",
        "elasticache:describeServiceUpdates",
        "elasticache:describeSnapshots",
        "elasticache:describeUpdateActions",
        "elasticache:describeUserGroups",
        "elasticache:describeUsers",
        "elasticache:listAllowedNodeTypeModifications",
        "elasticache:listTagsForResource",
        "elasticbeanstalk:checkDNSAvailability",
        "elasticbeanstalk:describeAccountAttributes",
        "elasticbeanstalk:describeApplicationVersions",
        "elasticbeanstalk:describeApplications",
        "elasticbeanstalk:describeConfigurationOptions",
        "elasticbeanstalk:describeEnvironmentHealth",
        "elasticbeanstalk:describeEnvironmentManagedActionHistory",
        "elasticbeanstalk:describeEnvironmentManagedActions",
        "elasticbeanstalk:describeEnvironmentResources",
        "elasticbeanstalk:describeEnvironments",
        "elasticbeanstalk:describeEvents",
        "elasticbeanstalk:describeInstancesHealth",
        "elasticbeanstalk:describePlatformVersion",
        "elasticbeanstalk:listAvailableSolutionStacks",
        "elasticbeanstalk:listPlatformBranches",
        "elasticbeanstalk:listPlatformVersions",
        "elasticbeanstalk:validateConfigurationSettings",
        "elasticfilesystem:describeAccessPoints",
        "elasticfilesystem:describeFileSystemPolicy",
        "elasticfilesystem:describeFileSystems",
        "elasticfilesystem:describeLifecycleConfiguration",
        "elasticfilesystem:describeMountTargets",
        "elasticfilesystem:describeMountTargetSecurityGroups",
        "elasticfilesystem:describeTags",
        "elasticfilesystem:listTagsForResource",
        "elasticloadbalancing:describeAccountLimits",
        "elasticloadbalancing:describeInstanceHealth",
        "elasticloadbalancing:describeListenerCertificates",
        "elasticloadbalancing:describeListeners",
        "elasticloadbalancing:describeLoadBalancerAttributes",
        "elasticloadbalancing:describeLoadBalancerPolicies",
        "elasticloadbalancing:describeLoadBalancerPolicyTypes",
        "elasticloadbalancing:describeLoadBalancers",
        "elasticloadbalancing:describeRules",
        "elasticloadbalancing:describeSSLPolicies",
```

```
        "elasticloadbalancing:describeTags",
        "elasticloadbalancing:describeTargetGroupAttributes",
        "elasticloadbalancing:describeTargetGroups",
        "elasticloadbalancing:describeTargetHealth",
        "elasticmapreduce:describeCluster",
        "elasticmapreduce:describeNotebookExecution",
        "elasticmapreduce:describeReleaseLabel",
        "elasticmapreduce:describeSecurityConfiguration",
        "elasticmapreduce:describeStep",
        "elasticmapreduce:describeStudio",
        "elasticmapreduce:getAutoTerminationPolicy",
        "elasticmapreduce:getBlockPublicAccessConfiguration",
        "elasticmapreduce:getManagedScalingPolicy",
        "elasticmapreduce:getStudioSessionMapping",
        "elasticmapreduce:listBootstrapActions",
        "elasticmapreduce:listClusters",
        "elasticmapreduce:listInstanceFleets",
        "elasticmapreduce:listInstanceGroups",
        "elasticmapreduce:listInstances",
        "elasticmapreduce:listNotebookExecutions",
        "elasticmapreduce:listReleaseLabels",
        "elasticmapreduce:listSecurityConfigurations",
        "elasticmapreduce:listSteps",
        "elasticmapreduce:listStudios",
        "elasticmapreduce:listStudioSessionMappings",
        "elastictranscoder:listJobsByPipeline",
        "elastictranscoder:listJobsByStatus",
        "elastictranscoder:listPipelines",
        "elastictranscoder:listPresets",
        "elastictranscoder:readPipeline",
        "elastictranscoder:readPreset",
        "emr-containers:describeJobRun",
        "emr-containers:describeJobTemplate",
        "emr-containers:describeManagedEndpoint",
        "emr-containers:describeVirtualCluster",
        "emr-containers:listJobRuns",
        "emr-containers:listJobTemplates",
        "emr-containers:listManagedEndpoints",
        "emr-containers:listVirtualClusters",
        "emr-serverless:getApplication",
        "emr-serverless:getJobRun",
        "emr-serverless:listApplications",
        "es:describeDomain",
        "es:describeDomainAutoTunes",
```

```
        "es:describeDomainChangeProgress",
        "es:describeDomainConfig",
        "es:describeDomains",
        "es:describeDryRunProgress",
        "es:describeElasticsearchDomain",
        "es:describeElasticsearchDomainConfig",
        "es:describeElasticsearchDomains",
        "es:describeInboundConnections",
        "es:describeInstanceTypeLimits",
        "es:describeOutboundConnections",
        "es:describePackages",
        "es:describeReservedInstanceOfferings",
        "es:describeReservedInstances",
        "es:describeVpcEndpoints",
        "es:getCompatibleVersions",
        "es:getPackageVersionHistory",
        "es:getUpgradeHistory",
        "es:getUpgradeStatus",
        "es:listDomainNames",
        "es:listDomainsForPackage",
        "es:listInstanceTypeDetails",
        "es:listPackagesForDomain",
        "es:listScheduledActions",
        "es:listTags",
        "es:listVersions",
        "es:listVpcEndpointAccess",
        "es:listVpcEndpoints",
        "es:listVpcEndpointsForDomain",
        "evidently:getExperiment",
        "evidently:getFeature",
        "evidently:getLaunch",
        "evidently:getProject",
        "evidently:getSegment",
        "evidently:listExperiments",
        "evidently:listFeatures",
        "evidently:listLaunches",
        "evidently:listProjects",
        "evidently:listSegments",
        "evidently:listSegmentReferences",
        "events:describeApiDestination",
        "events:describeArchive",
        "events:describeConnection",
        "events:describeEndpoint",
        "events:describeEventBus",
```

```
        "events:describeEventSource",
        "events:describePartnerEventSource",
        "events:describeReplay",
        "events:describeRule",
        "events:listArchives",
        "events:listApiDestinations",
        "events:listConnections",
        "events:listEndpoints",
        "events:listEventBuses",
        "events:listEventSources",
        "events:listPartnerEventSourceAccounts",
        "events:listPartnerEventSources",
        "events:listReplays",
        "events:listRuleNamesByTarget",
        "events:listRules",
        "events:listTargetsByRule",
        "events:testEventPattern",
        "firehose:describeDeliveryStream",
        "firehose:listDeliveryStreams",
        "fms:getAdminAccount",
        "fms:getComplianceDetail",
        "fms:getNotificationChannel",
        "fms:getPolicy",
        "fms:getProtectionStatus",
        "fms:listComplianceStatus",
        "fms:listMemberAccounts",
        "fms:listPolicies",
        "forecast:describeDataset",
        "forecast:describeDatasetGroup",
        "forecast:describeDatasetImportJob",
        "forecast:describeForecast",
        "forecast:describeForecastExportJob",
        "forecast:describePredictor",
        "forecast:getAccuracyMetrics",
        "forecast:listDatasetGroups",
        "forecast:listDatasetImportJobs",
        "forecast:listDatasets",
        "forecast:listForecastExportJobs",
        "forecast:listForecasts",
        "forecast:listPredictors",
        "fsx:describeBackups",
        "fsx:describeDataRepositoryAssociations",
        "fsx:describeDataRepositoryTasks",
        "fsx:describeFileCaches",
```

```
        "fsx:describeFileSystems",
        "fsx:describeSnapshots",
        "fsx:describeStorageVirtualMachines",
        "fsx:describeVolumes",
        "fsx:listTagsForResource",
        "gamelift:describeAlias",
        "gamelift:describeBuild",
        "gamelift:describeEC2InstanceLimits",
        "gamelift:describeFleetAttributes",
        "gamelift:describeFleetCapacity",
        "gamelift:describeFleetEvents",
        "gamelift:describeFleetLocationAttributes",
        "gamelift:describeFleetLocationCapacity",
        "gamelift:describeFleetLocationUtilization",
        "gamelift:describeFleetPortSettings",
        "gamelift:describeFleetUtilization",
        "gamelift:describeGameServer",
        "gamelift:describeGameServerGroup",
        "gamelift:describeGameSessionDetails",
        "gamelift:describeGameSessionPlacement",
        "gamelift:describeGameSessionQueues",
        "gamelift:describeGameSessions",
        "gamelift:describeInstances",
        "gamelift:describeMatchmaking",
        "gamelift:describeMatchmakingConfigurations",
        "gamelift:describeMatchmakingRuleSets",
        "gamelift:describePlayerSessions",
        "gamelift:describeRuntimeConfiguration",
        "gamelift:describeScalingPolicies",
        "gamelift:describeScript",
        "gamelift:listAliases",
        "gamelift:listBuilds",
        "gamelift:listFleets",
        "gamelift:listGameServerGroups",
        "gamelift:listGameServers",
        "gamelift:listScripts",
        "gamelift:resolveAlias",
        "glacier:describeJob",
        "glacier:describeVault",
        "glacier:getDataRetrievalPolicy",
        "glacier:getVaultAccessPolicy",
        "glacier:getVaultLock",
        "glacier:getVaultNotifications",
        "glacier:listJobs",
```

```
        "glacier:listTagsForVault",
        "glacier:listVaults",
        "globalaccelerator:describeAccelerator",
        "globalaccelerator:describeAcceleratorAttributes",
        "globalaccelerator:describeEndpointGroup",
        "globalaccelerator:describeListener",
        "globalaccelerator:listAccelerators",
        "globalaccelerator:listEndpointGroups",
        "globalaccelerator:listListeners",
        "glue:batchGetBlueprints",
        "glue:batchGetCrawlers",
        "glue:batchGetDevEndpoints",
        "glue:batchGetJobs",
        "glue:batchGetPartition",
        "glue:batchGetTriggers",
        "glue:batchGetWorkflows",
        "glue:checkSchemaVersionValidity",
        "glue:getBlueprint",
        "glue:getBlueprintRun",
        "glue:getBlueprintRuns",
        "glue:getCatalogImportStatus",
        "glue:getClassifier",
        "glue:getClassifiers",
        "glue:getColumnStatisticsForPartition",
        "glue:getColumnStatisticsForTable",
        "glue:getCrawler",
        "glue:getCrawlerMetrics",
        "glue:getCrawlers",
        "glue:getCustomEntityType",
        "glue:getDatabase",
        "glue:getDatabases",
        "glue:getDataflowGraph",
        "glue:getDataQualityResult",
        "glue:getDataQualityRuleRecommendationRun",
        "glue:getDataQualityRuleset",
        "glue:getDataQualityRulesetEvaluationRun",
        "glue:getDevEndpoint",
        "glue:getDevEndpoints",
        "glue:getJob",
        "glue:getJobRun",
        "glue:getJobRuns",
        "glue:getJobs",
        "glue:getMapping",
        "glue:getMLTaskRun",
```

```
        "glue:getMLTaskRuns",
        "glue:getMLTransform",
        "glue:getMLTransforms",
        "glue:getPartition",
        "glue:getPartitionIndexes",
        "glue:getPartitions",
        "glue:getRegistry",
        "glue:getResourcePolicies",
        "glue:getResourcePolicy",
        "glue:getSchema",
        "glue:getSchemaByDefinition",
        "glue:getSchemaVersion",
        "glue:getSchemaVersionsDiff",
        "glue:getSession",
        "glue:getStatement",
        "glue:getTable",
        "glue:getTables",
        "glue:getTableVersions",
        "glue:getTrigger",
        "glue:getTriggers",
        "glue:getUserDefinedFunction",
        "glue:getUserDefinedFunctions",
        "glue:getWorkflow",
        "glue:getWorkflowRun",
        "glue:getWorkflowRuns",
        "glue:listCrawlers",
        "glue:listCrawls",
        "glue:listDataQualityResults",
        "glue:listDataQualityRuleRecommendationRuns",
        "glue:listDataQualityRulesetEvaluationRuns",
        "glue:listDataQualityRulesets",
        "glue:listDevEndpoints",
        "glue:listMLTransforms",
        "glue:listRegistries",
        "glue:listSchemas",
        "glue:listSchemaVersions",
        "glue:listSessions",
        "glue:listStatements",
        "glue:querySchemaVersionMetadata",
        "greengrass:getConnectivityInfo",
        "greengrass:getCoreDefinition",
        "greengrass:getCoreDefinitionVersion",
        "greengrass:getDeploymentStatus",
        "greengrass:getDeviceDefinition",
```

```
        "greengrass:getDeviceDefinitionVersion",
        "greengrass:getFunctionDefinition",
        "greengrass:getFunctionDefinitionVersion",
        "greengrass:getGroup",
        "greengrass:getGroupCertificateAuthority",
        "greengrass:getGroupVersion",
        "greengrass:getLoggerDefinition",
        "greengrass:getLoggerDefinitionVersion",
        "greengrass:getResourceDefinitionVersion",
        "greengrass:getServiceRoleForAccount",
        "greengrass:getSubscriptionDefinition",
        "greengrass:getSubscriptionDefinitionVersion",
        "greengrass:listCoreDefinitions",
        "greengrass:listCoreDefinitionVersions",
        "greengrass:listDeployments",
        "greengrass:listDeviceDefinitions",
        "greengrass:listDeviceDefinitionVersions",
        "greengrass:listFunctionDefinitions",
        "greengrass:listFunctionDefinitionVersions",
        "greengrass:listGroups",
        "greengrass:listGroupVersions",
        "greengrass:listLoggerDefinitions",
        "greengrass:listLoggerDefinitionVersions",
        "greengrass:listResourceDefinitions",
        "greengrass:listResourceDefinitionVersions",
        "greengrass:listSubscriptionDefinitions",
        "greengrass:listSubscriptionDefinitionVersions",
        "guardduty:getDetector",
        "guardduty:getFindings",
        "guardduty:getFindingsStatistics",
        "guardduty:getInvitationsCount",
        "guardduty:getIPSet",
        "guardduty:getMasterAccount",
        "guardduty:getMembers",
        "guardduty:getThreatIntelSet",
        "guardduty:listDetectors",
        "guardduty:listFindings",
        "guardduty:listInvitations",
        "guardduty:listIPSets",
        "guardduty:listMembers",
        "guardduty:listThreatIntelSets",
        "health:describeAffectedAccountsForOrganization",
        "health:describeAffectedEntities",
        "health:describeAffectedEntitiesForOrganization",
```

```
        "health:describeEntityAggregates",
        "health:describeEntityAggregatesForOrganization",
        "health:describeEventAggregates",
        "health:describeEventDetails",
        "health:describeEventDetailsForOrganization",
        "health:describeEvents",
        "health:describeEventsForOrganization",
        "health:describeEventTypes",
        "health:describeHealthServiceStatusForOrganization",
        "iam:getAccessKeyLastUsed",
        "iam:getAccountAuthorizationDetails",
        "iam:getAccountPasswordPolicy",
        "iam:getAccountSummary",
        "iam:getContextKeysForCustomPolicy",
        "iam:getContextKeysForPrincipalPolicy",
        "iam:getCredentialReport",
        "iam:getGroup",
        "iam:getGroupPolicy",
        "iam:getInstanceProfile",
        "iam:getLoginProfile",
        "iam:getOpenIDConnectProvider",
        "iam:getPolicy",
        "iam:getPolicyVersion",
        "iam:getRole",
        "iam:getRolePolicy",
        "iam:getSAMLProvider",
        "iam:getServerCertificate",
        "iam:getServiceLinkedRoleDeletionStatus",
        "iam:getSSHPublicKey",
        "iam:getUser",
        "iam:getUserPolicy",
        "iam:listAccessKeys",
        "iam:listAccountAliases",
        "iam:listAttachedGroupPolicies",
        "iam:listAttachedRolePolicies",
        "iam:listAttachedUserPolicies",
        "iam:listEntitiesForPolicy",
        "iam:listGroupPolicies",
        "iam:listGroups",
        "iam:listGroupsForUser",
        "iam:listInstanceProfiles",
        "iam:listInstanceProfilesForRole",
        "iam:listMFADevices",
        "iam:listOpenIDConnectProviders",
```

```
        "iam:listPolicies",
        "iam:listPolicyVersions",
        "iam:listRolePolicies",
        "iam:listRoles",
        "iam:listSAMLProviders",
        "iam:listServerCertificates",
        "iam:listSigningCertificates",
        "iam:listSSHPublicKeys",
        "iam:listUserPolicies",
        "iam:listUsers",
        "iam:listVirtualMFADevices",
        "iam:simulateCustomPolicy",
        "iam:simulatePrincipalPolicy",
        "imagebuilder:getComponent",
        "imagebuilder:getComponentPolicy",
        "imagebuilder:getContainerRecipe",
        "imagebuilder:getDistributionConfiguration",
        "imagebuilder:getImage",
        "imagebuilder:getImagePipeline",
        "imagebuilder:getImagePolicy",
        "imagebuilder:getImageRecipe",
        "imagebuilder:getImageRecipePolicy",
        "imagebuilder:getInfrastructureConfiguration",
        "imagebuilder:getLifecycleExecution",
        "imagebuilder:getLifecyclePolicy",
        "imagebuilder:getWorkflowExecution",
        "imagebuilder:getWorkflowStepExecution",
        "imagebuilder:listComponentBuildVersions",
        "imagebuilder:listComponents",
        "imagebuilder:listContainerRecipes",
        "imagebuilder:listDistributionConfigurations",
        "imagebuilder:listImageBuildVersions",
        "imagebuilder:listImagePipelineImages",
        "imagebuilder:listImagePipelines",
        "imagebuilder:listImageRecipes",
        "imagebuilder:listImages",
        "imagebuilder:listImageScanFindingAggregations",
        "imagebuilder:listInfrastructureConfigurations",
        "imagebuilder:listLifecycleExecutions",
        "imagebuilder:listLifecycleExecutionResources",
        "imagebuilder:listLifecyclePolicies",
        "imagebuilder:listWorkflowExecutions",
        "imagebuilder:listWorkflowStepExecutions",
        "imagebuilder:listTagsForResource",
```

```
        "inspector:describeAssessmentRuns",
        "inspector:describeAssessmentTargets",
        "inspector:describeAssessmentTemplates",
        "inspector:describeCrossAccountAccessRole",
        "inspector:describeResourceGroups",
        "inspector:describeRulesPackages",
        "inspector:getTelemetryMetadata",
        "inspector:listAssessmentRunAgents",
        "inspector:listAssessmentRuns",
        "inspector:listAssessmentTargets",
        "inspector:listAssessmentTemplates",
        "inspector:listEventSubscriptions",
        "inspector:listRulesPackages",
        "inspector:listTagsForResource",
        "inspector2:batchGetAccountStatus",
        "inspector2:batchGetFreeTrialInfo",
        "inspector2:describeOrganizationConfiguration",
        "inspector2:getDelegatedAdminAccount",
        "inspector2:getMember",
        "inspector2:getSbomExport",
        "inspector2:listCoverage",
        "inspector2:listDelegatedAdminAccounts",
        "inspector2:listFilters",
        "inspector2:listFindings",
        "inspector2:listMembers",
        "inspector2:listUsageTotals",
        "inspector-scan:scanSbom",
        "internetmonitor:getMonitor",
        "internetmonitor:listMonitors",
        "internetmonitor:getHealthEvent",
        "internetmonitor:listHealthEvents",
        "iot:describeAuthorizer",
        "iot:describeCACertificate",
        "iot:describeCertificate",
        "iot:describeDefaultAuthorizer",
        "iot:describeDomainConfiguration",
        "iot:describeEndpoint",
        "iot:describeIndex",
        "iot:describeJobExecution",
        "iot:describeThing",
        "iot:describeThingGroup",
        "iot:describeTunnel",
        "iot:getEffectivePolicies",
        "iot:getIndexingConfiguration",
```

```
        "iot:getLoggingOptions",
        "iot:getPolicy",
        "iot:getPolicyVersion",
        "iot:getTopicRule",
        "iot:getV2LoggingOptions",
        "iot:listAttachedPolicies",
        "iot:listAuthorizers",
        "iot:listCACertificates",
        "iot:listCertificates",
        "iot:listCertificatesByCA",
        "iot:listDomainConfigurations",
        "iot:listJobExecutionsForJob",
        "iot:listJobExecutionsForThing",
        "iot:listJobs",
        "iot:listNamedShadowsForThing",
        "iot:listOutgoingCertificates",
        "iot:listPackages",
        "iot:listPackageVersions",
        "iot:listPolicies",
        "iot:listPolicyPrincipals",
        "iot:listPolicyVersions",
        "iot:listPrincipalPolicies",
        "iot:listPrincipalThings",
        "iot:listRoleAliases",
        "iot:listTargetsForPolicy",
        "iot:listThingGroups",
        "iot:listThingGroupsForThing",
        "iot:listThingPrincipals",
        "iot:listThingRegistrationTasks",
        "iot:listThings",
        "iot:listThingsInThingGroup",
        "iot:listThingTypes",
        "iot:listTopicRules",
        "iot:listTunnels",
        "iot:listV2LoggingLevels",
        "iotevents:describeDetector",
        "iotevents:describeDetectorModel",
        "iotevents:describeInput",
        "iotevents:describeLoggingOptions",
        "iotevents:listDetectorModels",
        "iotevents:listDetectorModelVersions",
        "iotevents:listDetectors",
        "iotevents:listInputs",
        "iotfleetwise:getCampaign",
```

```
        "iotfleetwise:getDecoderManifest",
        "iotfleetwise:getFleet",
        "iotfleetwise:getModelManifest",
        "iotfleetwise:getSignalCatalog",
        "iotfleetwise:getVehicle",
        "iotfleetwise:getVehicleStatus",
        "iotfleetwise:listCampaigns",
        "iotfleetwise:listDecoderManifests",
        "iotfleetwise:listDecoderManifestNetworkInterfaces",
        "iotfleetwise:listDecoderManifestSignals",
        "iotfleetwise:listFleets",
        "iotfleetwise:listFleetsForVehicle",
        "iotfleetwise:listModelManifests",
        "iotfleetwise:listModelManifestNodes",
        "iotfleetwise:listSignalCatalogs",
        "iotfleetwise:listSignalCatalogNodes",
        "iotfleetwise:listVehicles",
        "iotsitewise:describeAccessPolicy",
        "iotsitewise:describeAsset",
        "iotsitewise:describeAssetModel",
        "iotsitewise:describeAssetProperty",
        "iotsitewise:describeDashboard",
        "iotsitewise:describeGateway",
        "iotsitewise:describeGatewayCapabilityConfiguration",
        "iotsitewise:describeLoggingOptions",
        "iotsitewise:describePortal",
        "iotsitewise:describeProject",
        "iotsitewise:listAccessPolicies",
        "iotsitewise:listAssetModels",
        "iotsitewise:listAssets",
        "iotsitewise:listAssociatedAssets",
        "iotsitewise:listDashboards",
        "iotsitewise:listGateways",
        "iotsitewise:listPortals",
        "iotsitewise:listProjectAssets",
        "iotsitewise:listProjects",
        "iottwinmaker:getComponentType",
        "iottwinmaker:getEntity",
        "iottwinmaker:getPricingPlan",
        "iottwinmaker:getScene",
        "iottwinmaker:getWorkspace",
        "iottwinmaker:listComponentTypes",
        "iottwinmaker:listEntities",
        "iottwinmaker:listScenes",
```

```
        "iottwinmaker:getSyncJob",
        "iottwinmaker:listSyncJobs",
        "iottwinmaker:listSyncResources",
        "iottwinmaker:listWorkspaces",
        "iotwireless:getDestination",
        "iotwireless:getDeviceProfile",
        "iotwireless:getPartnerAccount",
        "iotwireless:getServiceEndpoint",
        "iotwireless:getServiceProfile",
        "iotwireless:getWirelessDevice",
        "iotwireless:getWirelessDeviceStatistics",
        "iotwireless:getWirelessGateway",
        "iotwireless:getWirelessGatewayCertificate",
        "iotwireless:getWirelessGatewayFirmwareInformation",
        "iotwireless:getWirelessGatewayStatistics",
        "iotwireless:getWirelessGatewayTask",
        "iotwireless:getWirelessGatewayTaskDefinition",
        "iotwireless:listDestinations",
        "iotwireless:listDeviceProfiles",
        "iotwireless:listPartnerAccounts",
        "iotwireless:listServiceProfiles",
        "iotwireless:listTagsForResource",
        "iotwireless:listWirelessDevices",
        "iotwireless:listWirelessGateways",
        "iotwireless:listWirelessGatewayTaskDefinitions",
        "ivs:getChannel",
        "ivs:getRecordingConfiguration",
        "ivs:getStream",
        "ivs:getStreamSession",
        "ivs:listChannels",
        "ivs:listPlaybackKeyPairs",
        "ivs:listRecordingConfigurations",
        "ivs:listStreamKeys",
        "ivs:listStreams",
        "ivs:listStreamSessions",
        "kafka:describeCluster",
        "kafka:describeClusterOperation",
        "kafka:describeClusterV2",
        "kafka:describeConfiguration",
        "kafka:describeConfigurationRevision",
        "kafka:getBootstrapBrokers",
        "kafka:listConfigurations",
        "kafka:listConfigurationRevisions",
        "kafka:listClusterOperations",
```

```
        "kafka:listClusters",
        "kafka:listClustersV2",
        "kafka:listNodes",
        "kafkaconnect:describeConnector",
        "kafkaconnect:describeCustomPlugin",
        "kafkaconnect:describeWorkerConfiguration",
        "kafkaconnect:listConnectors",
        "kafkaconnect:listCustomPlugins",
        "kafkaconnect:listWorkerConfigurations",
        "kendra:describeDataSource",
        "kendra:describeFaq",
        "kendra:describeIndex",
        "kendra:listDataSources",
        "kendra:listFaqs",
        "kendra:listIndices",
        "kinesis:describeStream",
        "kinesis:describeStreamConsumer",
        "kinesis:describeStreamSummary",
        "kinesis:listShards",
        "kinesis:listStreams",
        "kinesis:listStreamConsumers",
        "kinesis:listTagsForStream",
        "kinesisanalytics:describeApplication",
        "kinesisanalytics:describeApplicationSnapshot",
        "kinesisanalytics:listApplications",
        "kinesisanalytics:listApplicationSnapshots",
        "kinesisvideo:describeImageGenerationConfiguration",
        "kinesisvideo:describeNotificationConfiguration",
        "kinesisvideo:describeSignalingChannel",
        "kinesisvideo:describeStream",
        "kinesisvideo:getDataEndpoint",
        "kinesisvideo:getIceServerConfig",
        "kinesisvideo:getSignalingChannelEndpoint",
        "kinesisvideo:listSignalingChannels",
        "kinesisvideo:listStreams",
        "kms:describeKey",
        "kms:getKeyPolicy",
        "kms:getKeyRotationStatus",
        "kms:listAliases",
        "kms:listGrants",
        "kms:listKeyPolicies",
        "kms:listKeys",
        "kms:listResourceTags",
        "kms:listRetirableGrants",
```

```
        "lambda:getAccountSettings",
        "lambda:getAlias",
        "lambda:getCodeSigningConfig",
        "lambda:getEventSourceMapping",
        "lambda:getFunction",
        "lambda:getFunctionCodeSigningConfig",
        "lambda:getFunctionConcurrency",
        "lambda:getFunctionConfiguration",
        "lambda:getFunctionEventInvokeConfig",
        "lambda:getFunctionUrlConfig",
        "lambda:getLayerVersion",
        "lambda:getLayerVersionPolicy",
        "lambda:getPolicy",
        "lambda:getProvisionedConcurrencyConfig",
        "lambda:getRuntimeManagementConfig",
        "lambda:listAliases",
        "lambda:listCodeSigningConfigs",
        "lambda:listEventSourceMappings",
        "lambda:listFunctionEventInvokeConfigs",
        "lambda:listFunctions",
        "lambda:listFunctionsByCodeSigningConfig",
        "lambda:listFunctionUrlConfigs",
        "lambda:listLayers",
        "lambda:listLayerVersions",
        "lambda:listProvisionedConcurrencyConfigs",
        "lambda:listVersionsByFunction",
        "launchwizard:describeProvisionedApp",
        "launchwizard:describeProvisioningEvents",
        "launchwizard:listProvisionedApps",
        "lex:describeBot",
        "lex:describeBotAlias",
        "lex:describeBotLocale",
        "lex:describeBotRecommendation",
        "lex:describeBotVersion",
        "lex:describeCustomVocabularyMetadata",
        "lex:describeExport",
        "lex:describeImport",
        "lex:describeIntent",
        "lex:describeResourcePolicy",
        "lex:describeSlot",
        "lex:describeSlotType",
        "lex:getBot",
        "lex:getBotAlias",
        "lex:getBotAliases",
```

```
        "lex:getBotChannelAssociation",
        "lex:getBotChannelAssociations",
        "lex:getBots",
        "lex:getBotVersions",
        "lex:getBuiltinIntent",
        "lex:getBuiltinIntents",
        "lex:getBuiltinSlotTypes",
        "lex:getIntent",
        "lex:getIntents",
        "lex:getIntentVersions",
        "lex:getSlotType",
        "lex:getSlotTypes",
        "lex:getSlotTypeVersions",
        "lex:listBotAliases",
        "lex:listBotLocales",
        "lex:listBotRecommendations",
        "lex:listBots",
        "lex:listBotVersions",
        "lex:listExports",
        "lex:listImports",
        "lex:listIntents",
        "lex:listRecommendedIntents",
        "lex:listSlots",
        "lex:listSlotTypes",
        "license-manager:getLicenseConfiguration",
        "license-manager:getServiceSettings",
        "license-manager:listAssociationsForLicenseConfiguration",
        "license-manager:listFailuresForLicenseConfigurationOperations",
        "license-manager:listLicenseConfigurations",
        "license-manager:listLicenseSpecificationsForResource",
        "license-manager:listResourceInventory",
        "license-manager:listUsageForLicenseConfiguration",
        "lightsail:getActiveNames",
        "lightsail:getAlarms",
        "lightsail:getAutoSnapshots",
        "lightsail:getBlueprints",
        "lightsail:getBucketBundles",
        "lightsail:getBucketMetricData",
        "lightsail:getBuckets",
        "lightsail:getBundles",
        "lightsail:getCertificates",
        "lightsail:getContainerImages",
        "lightsail:getContainerServiceDeployments",
        "lightsail:getContainerServiceMetricData",
```

```
        "lightsail:getContainerServicePowers",
        "lightsail:getContainerServices",
        "lightsail:getDisk",
        "lightsail:getDisks",
        "lightsail:getDiskSnapshot",
        "lightsail:getDiskSnapshots",
        "lightsail:getDistributionBundles",
        "lightsail:getDistributionMetricData",
        "lightsail:getDistributions",
        "lightsail:getDomain",
        "lightsail:getDomains",
        "lightsail:getExportSnapshotRecords",
        "lightsail:getInstance",
        "lightsail:getInstanceMetricData",
        "lightsail:getInstancePortStates",
        "lightsail:getInstances",
        "lightsail:getInstanceSnapshot",
        "lightsail:getInstanceSnapshots",
        "lightsail:getInstanceState",
        "lightsail:getKeyPair",
        "lightsail:getKeyPairs",
        "lightsail:getLoadBalancer",
        "lightsail:getLoadBalancerMetricData",
        "lightsail:getLoadBalancers",
        "lightsail:getLoadBalancerTlsCertificates",
        "lightsail:getOperation",
        "lightsail:getOperations",
        "lightsail:getOperationsForResource",
        "lightsail:getRegions",
        "lightsail:getRelationalDatabase",
        "lightsail:getRelationalDatabaseMetricData",
        "lightsail:getRelationalDatabases",
        "lightsail:getRelationalDatabaseSnapshot",
        "lightsail:getRelationalDatabaseSnapshots",
        "lightsail:getStaticIp",
        "lightsail:getStaticIps",
        "lightsail:isVpcPeered",
        "logs:describeAccountPolicies",
        "logs:describeDeliveries",
        "logs:describeDeliveryDestinations",
        "logs:describeDeliverySources",
        "logs:describeDestinations",
        "logs:describeExportTasks",
        "logs:describeLogGroups",
```

```
        "logs:describeLogStreams",
        "logs:describeMetricFilters",
        "logs:describeQueries",
        "logs:describeQueryDefinitions",
        "logs:describeResourcePolicies",
        "logs:describeSubscriptionFilters",
        "logs:getDataProtectionPolicy",
        "logs:getDelivery",
        "logs:getDeliveryDestination",
        "logs:getDeliveryDestinationPolicy",
        "logs:getDeliverySource",
        "logs:getLogDelivery",
        "logs:getLogGroupFields",
        "logs:listLogDeliveries",
        "logs:testMetricFilter",
        "lookoutequipment:describeDataIngestionJob",
        "lookoutequipment:describeDataset",
        "lookoutequipment:describeInferenceScheduler",
        "lookoutequipment:describeModel",
        "lookoutequipment:listDataIngestionJobs",
        "lookoutequipment:listDatasets",
        "lookoutequipment:listInferenceExecutions",
        "lookoutequipment:listInferenceSchedulers",
        "lookoutequipment:listModels",
        "lookoutmetrics:describeAlert",
        "lookoutmetrics:describeAnomalyDetectionExecutions",
        "lookoutmetrics:describeAnomalyDetector",
        "lookoutmetrics:describeMetricSet",
        "lookoutmetrics:getAnomalyGroup",
        "lookoutmetrics:getDataQualityMetrics",
        "lookoutmetrics:getFeedback",
        "lookoutmetrics:getSampleData",
        "lookoutmetrics:listAlerts",
        "lookoutmetrics:listAnomalyDetectors",
        "lookoutmetrics:listAnomalyGroupSummaries",
        "lookoutmetrics:listAnomalyGroupTimeSeries",
        "lookoutmetrics:listMetricSets",
        "lookoutmetrics:listTagsForResource",
        "machinelearning:describeBatchPredictions",
        "machinelearning:describeDataSources",
        "machinelearning:describeEvaluations",
        "machinelearning:describeMLModels",
        "machinelearning:getBatchPrediction",
        "machinelearning:getDataSource",
```

```
        "machinelearning:getEvaluation",
        "machinelearning:getMLModel",
        "macie2:getClassificationExportConfiguration",
        "macie2:getCustomDataIdentifier",
        "macie2:getFindings",
        "macie2:getFindingStatistics",
        "macie2:listClassificationJobs",
        "macie2:listCustomDataIdentifiers",
        "macie2:listFindings",
        "managedblockchain:getMember",
        "managedblockchain:getNetwork",
        "managedblockchain:getNode",
        "managedblockchain:listMembers",
        "managedblockchain:listNetworks",
        "managedblockchain:listNodes",
        "mediaconnect:describeFlow",
        "mediaconnect:listEntitlements",
        "mediaconnect:listFlows",
        "mediaconvert:describeEndpoints",
        "mediaconvert:getJob",
        "mediaconvert:getJobTemplate",
        "mediaconvert:getPreset",
        "mediaconvert:getQueue",
        "mediaconvert:listJobs",
        "mediaconvert:listJobTemplates",
        "medialive:describeChannel",
        "medialive:describeInput",
        "medialive:describeInputDevice",
        "medialive:describeInputSecurityGroup",
        "medialive:describeMultiplex",
        "medialive:describeOffering",
        "medialive:describeReservation",
        "medialive:describeSchedule",
        "medialive:listChannels",
        "medialive:listInputDevices",
        "medialive:listInputs",
        "medialive:listInputSecurityGroups",
        "medialive:listMultiplexes",
        "medialive:listOfferings",
        "medialive:listReservations",
        "mediapackage:describeChannel",
        "mediapackage:describeOriginEndpoint",
        "mediapackage:listChannels",
        "mediapackage:listOriginEndpoints",
```

```
        "mediastore:describeContainer",
        "mediastore:getContainerPolicy",
        "mediastore:getCorsPolicy",
        "mediastore:listContainers",
        "mediatailor:getPlaybackConfiguration",
        "mediatailor:listPlaybackConfigurations",
        "medical-imaging:getDatastore",
        "medical-imaging:listDatastores",
        "mgn:describeJobLogItems",
        "mgn:describeJobs",
        "mgn:describeLaunchConfigurationTemplates",
        "mgn:describeReplicationConfigurationTemplates",
        "mgn:describeSourceServers",
        "mgn:describeVcenterClients",
        "mgn:getLaunchConfiguration",
        "mgn:getReplicationConfiguration",
        "mgn:listApplications",
        "mgn:listSourceServerActions",
        "mgn:listTemplateActions",
        "mgn:listWaves",
        "mobiletargeting:getAdmChannel",
        "mobiletargeting:getApnsChannel",
        "mobiletargeting:getApnsSandboxChannel",
        "mobiletargeting:getApnsVoipChannel",
        "mobiletargeting:getApnsVoipSandboxChannel",
        "mobiletargeting:getApp",
        "mobiletargeting:getApplicationSettings",
        "mobiletargeting:getApps",
        "mobiletargeting:getBaiduChannel",
        "mobiletargeting:getCampaign",
        "mobiletargeting:getCampaignActivities",
        "mobiletargeting:getCampaigns",
        "mobiletargeting:getCampaignVersion",
        "mobiletargeting:getCampaignVersions",
        "mobiletargeting:getEmailChannel",
        "mobiletargeting:getEndpoint",
        "mobiletargeting:getEventStream",
        "mobiletargeting:getExportJob",
        "mobiletargeting:getExportJobs",
        "mobiletargeting:getGcmChannel",
        "mobiletargeting:getImportJob",
        "mobiletargeting:getImportJobs",
        "mobiletargeting:getJourney",
        "mobiletargeting:getJourneyExecutionMetrics",
```

```
        "mobiletargeting:getJourneyExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionMetrics",
        "mobiletargeting:getJourneyRuns",
        "mobiletargeting:getSegment",
        "mobiletargeting:getSegmentImportJobs",
        "mobiletargeting:getSegments",
        "mobiletargeting:getSegmentVersion",
        "mobiletargeting:getSegmentVersions",
        "mobiletargeting:getSmsChannel",
        "mobiletargeting:listJourneys",
        "mq:describeBroker",
        "mq:describeConfiguration",
        "mq:describeConfigurationRevision",
        "mq:describeUser",
        "mq:listBrokers",
        "mq:listConfigurationRevisions",
        "mq:listConfigurations",
        "mq:listUsers",
        "m2:getApplication",
        "m2:getApplicationVersion",
        "m2:getBatchJobExecution",
        "m2:getDataSetDetails",
        "m2:getDataSetImportTask",
        "m2:getDeployment",
        "m2:getEnvironment",
        "m2:listApplications",
        "m2:listApplicationVersions",
        "m2:listBatchJobDefinitions",
        "m2:listBatchJobExecutions",
        "m2:listDataSetImportHistory",
        "m2:listDataSets",
        "m2:listDeployments",
        "m2:listEngineVersions",
        "m2:listEnvironments",
        "network-firewall:describeFirewall",
        "network-firewall:describeFirewallPolicy",
        "network-firewall:describeLoggingConfiguration",
        "network-firewall:describeRuleGroup",
        "network-firewall:describeTlsInspectionConfiguration",
        "network-firewall:listFirewallPolicies",
        "network-firewall:listFirewalls",
        "network-firewall:listRuleGroups",
        "network-firewall:listTlsInspectionConfigurations",
```

```
        "networkmanager:describeGlobalNetworks",
        "networkmanager:getConnectAttachment",
        "networkmanager:getConnections",
        "networkmanager:getConnectPeer",
        "networkmanager:getConnectPeerAssociations",
        "networkmanager:getCoreNetwork",
        "networkmanager:getCoreNetworkChangeEvents",
        "networkmanager:getCoreNetworkChangeSet",
        "networkmanager:getCoreNetworkPolicy",
        "networkmanager:getCustomerGatewayAssociations",
        "networkmanager:getDevices",
        "networkmanager:getLinkAssociations",
        "networkmanager:getLinks",
        "networkmanager:getNetworkResourceCounts",
        "networkmanager:getNetworkResourceRelationships",
        "networkmanager:getNetworkResources",
        "networkmanager:getNetworkRoutes",
        "networkmanager:getNetworkTelemetry",
        "networkmanager:getResourcePolicy",
        "networkmanager:getRouteAnalysis",
        "networkmanager:getSites",
        "networkmanager:getSiteToSiteVpnAttachment",
        "networkmanager:getTransitGatewayConnectPeerAssociations",
        "networkmanager:getTransitGatewayPeering",
        "networkmanager:getTransitGatewayRegistrations",
        "networkmanager:getTransitGatewayRouteTableAttachment",
        "networkmanager:getVpcAttachment",
        "networkmanager:listAttachments",
        "networkmanager:listConnectPeers",
        "networkmanager:listCoreNetworkPolicyVersions",
        "networkmanager:listCoreNetworks",
        "networkmanager:listOrganizationServiceAccessStatus",
        "networkmanager:listPeerings",
        "networkmanager:listTagsForResource",
        "nimble:getEula",
        "nimble:getLaunchProfile",
        "nimble:getLaunchProfileDetails",
        "nimble:getLaunchProfileInitialization",
        "nimble:getLaunchProfileMember",
        "nimble:getStreamingImage",
        "nimble:getStreamingSession",
        "nimble:getStreamingSessionStream",
        "nimble:getStudio",
        "nimble:getStudioComponent",
```

```
        "nimble:listEulaAcceptances",
        "nimble:listEulas",
        "nimble:listLaunchProfiles",
        "nimble:listStreamingImages",
        "nimble:listStreamingSessions",
        "nimble:listStudioComponents",
        "nimble:listStudios",
        "notifications:getEventRule",
        "notifications:getNotificationConfiguration",
        "notifications:getNotificationEvent",
        "notifications:listChannels",
        "notifications:listEventRules",
        "notifications:listNotificationConfigurations",
        "notifications:listNotificationEvents",
        "notifications:listNotificationHubs",
        "notifications-contacts:getEmailContact",
        "notifications-contacts:listEmailContacts",
        "oam:getLink",
        "oam:getSink",
        "oam:getSinkPolicy",
        "oam:listAttachedLinks",
        "oam:listLinks",
        "oam:listSinks",
        "omics:getAnnotationImportJob",
        "omics:getAnnotationStore",
        "omics:getReadSetImportJob",
        "omics:getReadSetMetadata",
        "omics:getReference",
        "omics:getReferenceImportJob",
        "omics:getReferenceMetadata",
        "omics:getReferenceStore",
        "omics:getRun",
        "omics:getRunGroup",
        "omics:getSequenceStore",
        "omics:getVariantImportJob",
        "omics:getVariantStore",
        "omics:getWorkflow",
        "omics:listAnnotationImportJobs",
        "omics:listAnnotationStores",
        "omics:listMultipartReadSetUploads",
        "omics:listReadSetImportJobs",
        "omics:listReadSets",
        "omics:listReadSetUploadParts",
        "omics:listReferenceImportJobs",
```

```
        "omics:listReferenceStores",
        "omics:listReferences",
        "omics:listRunGroups",
        "omics:listRunTasks",
        "omics:listRuns",
        "omics:listSequenceStores",
        "omics:listVariantImportJobs",
        "omics:listVariantStores",
        "omics:listWorkflows",
        "opsworks-cm:describeAccountAttributes",
        "opsworks-cm:describeBackups",
        "opsworks-cm:describeEvents",
        "opsworks-cm:describeNodeAssociationStatus",
        "opsworks-cm:describeServers",
        "opsworks:describeAgentVersions",
        "opsworks:describeApps",
        "opsworks:describeCommands",
        "opsworks:describeDeployments",
        "opsworks:describeEcsClusters",
        "opsworks:describeElasticIps",
        "opsworks:describeElasticLoadBalancers",
        "opsworks:describeInstances",
        "opsworks:describeLayers",
        "opsworks:describeLoadBasedAutoScaling",
        "opsworks:describeMyUserProfile",
        "opsworks:describePermissions",
        "opsworks:describeRaidArrays",
        "opsworks:describeRdsDbInstances",
        "opsworks:describeServiceErrors",
        "opsworks:describeStackProvisioningParameters",
        "opsworks:describeStacks",
        "opsworks:describeStackSummary",
        "opsworks:describeTimeBasedAutoScaling",
        "opsworks:describeUserProfiles",
        "opsworks:describeVolumes",
        "opsworks:getHostnameSuggestion",
        "organizations:listAccounts",
        "organizations:listTagsForResource",
        "outposts:getCatalogItem",
        "outposts:getConnection",
        "outposts:getOrder",
        "outposts:getOutpost",
        "outposts:getOutpostInstanceTypes",
        "outposts:getSite",
```

```
        "outposts:listAssets",
        "outposts:listCatalogItems",
        "outposts:listOrders",
        "outposts:listOutposts",
        "outposts:listSites",
        "personalize:describeAlgorithm",
        "personalize:describeBatchInferenceJob",
        "personalize:describeBatchSegmentJob",
        "personalize:describeCampaign",
        "personalize:describeDataset",
        "personalize:describeDatasetExportJob",
        "personalize:describeDatasetGroup",
        "personalize:describeDatasetImportJob",
        "personalize:describeEventTracker",
        "personalize:describeFeatureTransformation",
        "personalize:describeFilter",
        "personalize:describeRecipe",
        "personalize:describeRecommender",
        "personalize:describeSchema",
        "personalize:describeSolution",
        "personalize:describeSolutionVersion",
        "personalize:getPersonalizedRanking",
        "personalize:getRecommendations",
        "personalize:getSolutionMetrics",
        "personalize:listBatchInferenceJobs",
        "personalize:listBatchSegmentJobs",
        "personalize:listCampaigns",
        "personalize:listDatasetExportJobs",
        "personalize:listDatasetGroups",
        "personalize:listDatasetImportJobs",
        "personalize:listDatasets",
        "personalize:listEventTrackers",
        "personalize:listRecipes",
        "personalize:listRecommenders",
        "personalize:listSchemas",
        "personalize:listSolutions",
        "personalize:listSolutionVersions",
        "pipes:describePipe",
        "pipes:listPipes",
        "pipes:listTagsForResource",
        "polly:describeVoices",
        "polly:getLexicon",
        "polly:listLexicons",
        "pricing:describeServices",
```

```
        "pricing:getAttributeValues",
        "pricing:getProducts",
        "private-networks:getDeviceIdentifier",
        "private-networks:getNetwork",
        "private-networks:getNetworkResource",
        "private-networks:listDeviceIdentifiers",
        "private-networks:listNetworks",
        "private-networks:listNetworkResources",
        "quicksight:describeAccountCustomization",
        "quicksight:describeAccountSettings",
        "quicksight:describeAccountSubscription",
        "quicksight:describeAnalysis",
        "quicksight:describeAnalysisPermissions",
        "quicksight:describeDashboard",
        "quicksight:describeDashboardPermissions",
        "quicksight:describeDataSet",
        "quicksight:describeDataSetPermissions",
        "quicksight:describeDataSetRefreshProperties",
        "quicksight:describeDataSource",
        "quicksight:describeDataSourcePermissions",
        "quicksight:describeFolder",
        "quicksight:describeFolderPermissions",
        "quicksight:describeFolderResolvedPermissions",
        "quicksight:describeGroup",
        "quicksight:describeGroupMembership",
        "quicksight:describeIAMPolicyAssignment",
        "quicksight:describeIngestion",
        "quicksight:describeIpRestriction",
        "quicksight:describeNamespace",
        "quicksight:describeRefreshSchedule",
        "quicksight:describeTemplate",
        "quicksight:describeTemplateAlias",
        "quicksight:describeTemplatePermissions",
        "quicksight:describeTheme",
        "quicksight:describeThemeAlias",
        "quicksight:describeThemePermissions",
        "quicksight:describeTopic",
        "quicksight:describeTopicPermissions",
        "quicksight:describeTopicRefresh",
        "quicksight:describeTopicRefreshSchedule",
        "quicksight:describeUser",
        "quicksight:describeVPCConnection",
        "quicksight:listAnalyses",
        "quicksight:listDashboards",
```

```
        "quicksight:listDashboardVersions",
        "quicksight:listDataSets",
        "quicksight:listDataSources",
        "quicksight:listFolderMembers",
        "quicksight:listFolders",
        "quicksight:listGroupMemberships",
        "quicksight:listGroups",
        "quicksight:listIAMPolicyAssignments",
        "quicksight:listIAMPolicyAssignmentsForUser",
        "quicksight:listIngestions",
        "quicksight:listNamespaces",
        "quicksight:listRefreshSchedules",
        "quicksight:listTemplateAliases",
        "quicksight:listTemplates",
        "quicksight:listTemplateVersions",
        "quicksight:listThemeAliases",
        "quicksight:listThemes",
        "quicksight:listThemeVersions",
        "quicksight:listTopicRefreshSchedules",
        "quicksight:listTopics",
        "quicksight:listUserGroups",
        "quicksight:listUsers",
        "quicksight:listVPCConnections",
        "quicksight:searchAnalyses",
        "quicksight:searchDashboards",
        "quicksight:searchDataSets",
        "quicksight:searchDataSources",
        "quicksight:searchFolders",
        "quicksight:searchGroups",
        "ram:getPermission",
        "ram:getResourceShareAssociations",
        "ram:getResourceShareInvitations",
        "ram:getResourceShares",
        "ram:listPendingInvitationResources",
        "ram:listPrincipals",
        "ram:listResources",
        "ram:listResourceSharePermissions",
        "rbin:getRule",
        "rbin:listRules",
        "rds:describeAccountAttributes",
        "rds:describeBlueGreenDeployments",
        "rds:describeCertificates",
        "rds:describeDBClusterEndpoints",
        "rds:describeDBClusterParameterGroups",
```

```
        "rds:describeDBClusterParameters",
        "rds:describeDBClusters",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBEngineVersions",
        "rds:describeDBInstanceAutomatedBackups",
        "rds:describeDBInstances",
        "rds:describeDBLogFiles",
        "rds:describeDBParameterGroups",
        "rds:describeDBParameters",
        "rds:describeDBSecurityGroups",
        "rds:describeDBSnapshotAttributes",
        "rds:describeDBSnapshots",
        "rds:describeDBSubnetGroups",
        "rds:describeEngineDefaultClusterParameters",
        "rds:describeEngineDefaultParameters",
        "rds:describeEventCategories",
        "rds:describeEvents",
        "rds:describeEventSubscriptions",
        "rds:describeExportTasks",
        "rds:describeGlobalClusters",
        "rds:describeIntegrations",
        "rds:describeOptionGroupOptions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describePendingMaintenanceActions",
        "rds:describeReservedDBInstances",
        "rds:describeReservedDBInstancesOfferings",
        "rds:describeSourceRegions",
        "rds:describeValidDBInstanceModifications",
        "rds:listTagsForResource",
        "redshift-data:describeStatement",
        "redshift-data:listStatements",
        "redshift:describeClusterParameterGroups",
        "redshift:describeClusterParameters",
        "redshift:describeClusters",
        "redshift:describeClusterSecurityGroups",
        "redshift:describeClusterSnapshots",
        "redshift:describeClusterSubnetGroups",
        "redshift:describeClusterVersions",
        "redshift:describeDataShares",
        "redshift:describeDataSharesForConsumer",
        "redshift:describeDataSharesForProducer",
        "redshift:describeDefaultClusterParameters",
        "redshift:describeEventCategories",
```

```
        "redshift:describeEvents",
        "redshift:describeEventSubscriptions",
        "redshift:describeHsmClientCertificates",
        "redshift:describeHsmConfigurations",
        "redshift:describeLoggingStatus",
        "redshift:describeOrderableClusterOptions",
        "redshift:describeReservedNodeOfferings",
        "redshift:describeReservedNodes",
        "redshift:describeResize",
        "redshift:describeSnapshotCopyGrants",
        "redshift:describeStorage",
        "redshift:describeTableRestoreStatus",
        "redshift:describeTags",
        "redshift-serverless:getEndpointAccess",
        "redshift-serverless:getNamespace",
        "redshift-serverless:getRecoveryPoint",
        "redshift-serverless:getSnapshot",
        "redshift-serverless:getTableRestoreStatus",
        "redshift-serverless:getUsageLimit",
        "redshift-serverless:getWorkgroup",
        "redshift-serverless:listEndpointAccess",
        "redshift-serverless:listNamespaces",
        "redshift-serverless:listRecoveryPoints",
        "redshift-serverless:listSnapshots",
        "redshift-serverless:listTableRestoreStatus",
        "redshift-serverless:listUsageLimits",
        "redshift-serverless:listWorkgroups",
        "rekognition:listCollections",
        "rekognition:listFaces",
        "resource-explorer-2:getAccountLevelServiceConfiguration",
        "resource-explorer-2:getIndex",
        "resource-explorer-2:getView",
        "resource-explorer-2:listIndexes",
        "resource-explorer-2:listViews",
        "resource-explorer-2:search",
        "resource-groups:getGroup",
        "resource-groups:getGroupQuery",
        "resource-groups:getTags",
        "resource-groups:listGroupResources",
        "resource-groups:listGroups",
        "resource-groups:searchResources",
        "robomaker:batchDescribeSimulationJob",
        "robomaker:describeDeploymentJob",
        "robomaker:describeFleet",
```

```
        "robomaker:describeRobot",
        "robomaker:describeRobotApplication",
        "robomaker:describeSimulationApplication",
        "robomaker:describeSimulationJob",
        "robomaker:listDeploymentJobs",
        "robomaker:listFleets",
        "robomaker:listRobotApplications",
        "robomaker:listRobots",
        "robomaker:listSimulationApplications",
        "robomaker:listSimulationJobs",
        "route53-recovery-cluster:getRoutingControlState",
        "route53-recovery-cluster:listRoutingControls",
        "route53-recovery-control-config:describeControlPanel",
        "route53-recovery-control-config:describeRoutingControl",
        "route53-recovery-control-config:describeSafetyRule",
        "route53-recovery-control-config:listControlPanels",
        "route53-recovery-control-config:listRoutingControls",
        "route53-recovery-control-config:listSafetyRules",
        "route53-recovery-readiness:getCell",
        "route53-recovery-readiness:getCellReadinessSummary",
        "route53-recovery-readiness:getReadinessCheck",
        "route53-recovery-readiness:getReadinessCheckResourceStatus",
        "route53-recovery-readiness:getReadinessCheckStatus",
        "route53-recovery-readiness:getRecoveryGroup",
        "route53-recovery-readiness:getRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:listCells",
        "route53-recovery-readiness:listReadinessChecks",
        "route53-recovery-readiness:listRecoveryGroups",
        "route53-recovery-readiness:listResourceSets",
        "route53:getAccountLimit",
        "route53:getChange",
        "route53:getCheckerIpRanges",
        "route53:getDNSSEC",
        "route53:getGeoLocation",
        "route53:getHealthCheck",
        "route53:getHealthCheckCount",
        "route53:getHealthCheckLastFailureReason",
        "route53:getHealthCheckStatus",
        "route53:getHostedZone",
        "route53:getHostedZoneCount",
        "route53:getHostedZoneLimit",
        "route53:getQueryLoggingConfig",
        "route53:getReusableDelegationSet",
        "route53:getTrafficPolicy",
```

```
        "route53:getTrafficPolicyInstance",
        "route53:getTrafficPolicyInstanceCount",
        "route53:listCidrBlocks",
        "route53:listCidrCollections",
        "route53:listCidrLocations",
        "route53:listGeoLocations",
        "route53:listHealthChecks",
        "route53:listHostedZones",
        "route53:listHostedZonesByName",
        "route53:listHostedZonesByVpc",
        "route53:listQueryLoggingConfigs",
        "route53:listResourceRecordSets",
        "route53:listReusableDelegationSets",
        "route53:listTrafficPolicies",
        "route53:listTrafficPolicyInstances",
        "route53:listTrafficPolicyInstancesByHostedZone",
        "route53:listTrafficPolicyInstancesByPolicy",
        "route53:listTrafficPolicyVersions",
        "route53:listVPCAssociationAuthorizations",
        "route53domains:checkDomainAvailability",
        "route53domains:getContactReachabilityStatus",
        "route53domains:getDomainDetail",
        "route53domains:getOperationDetail",
        "route53domains:listDomains",
        "route53domains:listOperations",
        "route53domains:listPrices",
        "route53domains:listTagsForDomain",
        "route53domains:viewBilling",
        "route53resolver:getFirewallConfig",
        "route53resolver:getFirewallDomainList",
        "route53resolver:getFirewallRuleGroup",
        "route53resolver:getFirewallRuleGroupAssociation",
        "route53resolver:getFirewallRuleGroupPolicy",
        "route53resolver:getOutpostResolver",
        "route53resolver:getResolverDnssecConfig",
        "route53resolver:getResolverQueryLogConfig",
        "route53resolver:getResolverQueryLogConfigAssociation",
        "route53resolver:getResolverQueryLogConfigPolicy",
        "route53resolver:getResolverRule",
        "route53resolver:getResolverRuleAssociation",
        "route53resolver:getResolverRulePolicy",
        "route53resolver:listFirewallConfigs",
        "route53resolver:listFirewallDomainLists",
        "route53resolver:listFirewallDomains",
```

```
        "route53resolver:listFirewallRuleGroupAssociations",
        "route53resolver:listFirewallRuleGroups",
        "route53resolver:listFirewallRules",
        "route53resolver:listOutpostResolvers",
        "route53resolver:listResolverConfigs",
        "route53resolver:listResolverDnssecConfigs",
        "route53resolver:listResolverEndpointIpAddresses",
        "route53resolver:listResolverEndpoints",
        "route53resolver:listResolverQueryLogConfigAssociations",
        "route53resolver:listResolverQueryLogConfigs",
        "route53resolver:listResolverRuleAssociations",
        "route53resolver:listResolverRules",
        "route53resolver:listTagsForResource",
        "rum:batchGetRumMetricDefinitions",
        "rum:getAppMonitor",
        "rum:listAppMonitors",
        "rum:listRumMetricsDestinations",
        "s3:describeJob",
        "s3:describeMultiRegionAccessPointOperation",
        "s3:getAccelerateConfiguration",
        "s3:getAccessPoint",
        "s3:getAccessPointConfigurationForObjectLambda",
        "s3:getAccessPointForObjectLambda",
        "s3:getAccessPointPolicy",
        "s3:getAccessPointPolicyForObjectLambda",
        "s3:getAccessPointPolicyStatus",
        "s3:getAccessPointPolicyStatusForObjectLambda",
        "s3:getAccountPublicAccessBlock",
        "s3:getAnalyticsConfiguration",
        "s3:getBucketAcl",
        "s3:getBucketCORS",
        "s3:getBucketLocation",
        "s3:getBucketLogging",
        "s3:getBucketNotification",
        "s3:getBucketObjectLockConfiguration",
        "s3:getBucketOwnershipControls",
        "s3:getBucketPolicy",
        "s3:getBucketPolicyStatus",
        "s3:getBucketPublicAccessBlock",
        "s3:getBucketRequestPayment",
        "s3:getBucketVersioning",
        "s3:getBucketWebsite",
        "s3:getEncryptionConfiguration",
        "s3:getIntelligentTieringConfiguration",
```

```
        "s3:getInventoryConfiguration",
        "s3:getLifecycleConfiguration",
        "s3:getMetricsConfiguration",
        "s3:getMultiRegionAccessPoint",
        "s3:getMultiRegionAccessPointPolicy",
        "s3:getMultiRegionAccessPointPolicyStatus",
        "s3:getMultiRegionAccessPointRoutes",
        "s3:getObjectLegalHold",
        "s3:getObjectRetention",
        "s3:getReplicationConfiguration",
        "s3:getStorageLensConfiguration",
        "s3:listAccessPoints",
        "s3:listAccessPointsForObjectLambda",
        "s3:listAllMyBuckets",
        "s3:listBucket",
        "s3:listBucketMultipartUploads",
        "s3:listBucketVersions",
        "s3:listJobs",
        "s3:listMultipartUploadParts",
        "s3:listMultiRegionAccessPoints",
        "s3:listStorageLensConfigurations",
        "s3express:listAllMyDirectoryBuckets",
        "sagemaker:describeAction",
        "sagemaker:describeAlgorithm",
        "sagemaker:describeApp",
        "sagemaker:describeAppImageConfig",
        "sagemaker:describeArtifact",
        "sagemaker:describeAutoMLJob",
        "sagemaker:describeCodeRepository",
        "sagemaker:describeCompilationJob",
        "sagemaker:describeContext",
        "sagemaker:describeDataQualityJobDefinition",
        "sagemaker:describeDevice",
        "sagemaker:describeDeviceFleet",
        "sagemaker:describeDomain",
        "sagemaker:describeEdgeDeploymentPlan",
        "sagemaker:describeEdgePackagingJob",
        "sagemaker:describeEndpoint",
        "sagemaker:describeEndpointConfig",
        "sagemaker:describeExperiment",
        "sagemaker:describeFeatureGroup",
        "sagemaker:describeFeatureMetadata",
        "sagemaker:describeFlowDefinition",
        "sagemaker:describeHub",
```

```
        "sagemaker:describeHubContent",
        "sagemaker:describeHumanTaskUi",
        "sagemaker:describeHyperParameterTuningJob",
        "sagemaker:describeImage",
        "sagemaker:describeImageVersion",
        "sagemaker:describeInferenceExperiment",
        "sagemaker:describeInferenceRecommendationsJob",
        "sagemaker:describeLabelingJob",
        "sagemaker:describeModel",
        "sagemaker:describeModelBiasJobDefinition",
        "sagemaker:describeModelCard",
        "sagemaker:describeModelCardExportJob",
        "sagemaker:describeModelExplainabilityJobDefinition",
        "sagemaker:describeModelPackage",
        "sagemaker:describeModelPackageGroup",
        "sagemaker:describeModelQualityJobDefinition",
        "sagemaker:describeMonitoringSchedule",
        "sagemaker:describeNotebookInstance",
        "sagemaker:describeNotebookInstanceLifecycleConfig",
        "sagemaker:describePipeline",
        "sagemaker:describePipelineDefinitionForExecution",
        "sagemaker:describePipelineExecution",
        "sagemaker:describeProcessingJob",
        "sagemaker:describeProject",
        "sagemaker:describeSpace",
        "sagemaker:describeStudioLifecycleConfig",
        "sagemaker:describeSubscribedWorkteam",
        "sagemaker:describeTrainingJob",
        "sagemaker:describeTransformJob",
        "sagemaker:describeTrial",
        "sagemaker:describeTrialComponent",
        "sagemaker:describeUserProfile",
        "sagemaker:describeWorkforce",
        "sagemaker:describeWorkteam",
        "sagemaker:getDeviceFleetReport",
        "sagemaker:getModelPackageGroupPolicy",
        "sagemaker:getSagemakerServicecatalogPortfolioStatus",
        "sagemaker:listActions",
        "sagemaker:listAlgorithms",
        "sagemaker:listAliases",
        "sagemaker:listAppImageConfigs",
        "sagemaker:listApps",
        "sagemaker:listArtifacts",
        "sagemaker:listAssociations",
```

```
        "sagemaker:listAutoMLJobs",
        "sagemaker:listCandidatesForAutoMLJob",
        "sagemaker:listCodeRepositories",
        "sagemaker:listCompilationJobs",
        "sagemaker:listContexts",
        "sagemaker:listDataQualityJobDefinitions",
        "sagemaker:listDeviceFleets",
        "sagemaker:listDevices",
        "sagemaker:listDomains",
        "sagemaker:listEdgeDeploymentPlans",
        "sagemaker:listEdgePackagingJobs",
        "sagemaker:listEndpointConfigs",
        "sagemaker:listEndpoints",
        "sagemaker:listExperiments",
        "sagemaker:listFeatureGroups",
        "sagemaker:listFlowDefinitions",
        "sagemaker:listHubContents",
        "sagemaker:listHubContentVersions",
        "sagemaker:listHubs",
        "sagemaker:listHumanTaskUis",
        "sagemaker:listHyperParameterTuningJobs",
        "sagemaker:listImages",
        "sagemaker:listImageVersions",
        "sagemaker:listInferenceExperiments",
        "sagemaker:listInferenceRecommendationsJobs",
        "sagemaker:listInferenceRecommendationsJobSteps",
        "sagemaker:listLabelingJobs",
        "sagemaker:listLabelingJobsForWorkteam",
        "sagemaker:listLineageGroups",
        "sagemaker:listModelBiasJobDefinitions",
        "sagemaker:listModelCardExportJobs",
        "sagemaker:listModelCards",
        "sagemaker:listModelCardVersions",
        "sagemaker:listModelExplainabilityJobDefinitions",
        "sagemaker:listModelMetadata",
        "sagemaker:listModelPackageGroups",
        "sagemaker:listModelPackages",
        "sagemaker:listModelQualityJobDefinitions",
        "sagemaker:listModels",
        "sagemaker:listMonitoringAlertHistory",
        "sagemaker:listMonitoringAlerts",
        "sagemaker:listMonitoringExecutions",
        "sagemaker:listMonitoringSchedules",
        "sagemaker:listNotebookInstanceLifecycleConfigs",
```

```
        "sagemaker:listNotebookInstances",
        "sagemaker:listPipelineExecutions",
        "sagemaker:listPipelineExecutionSteps",
        "sagemaker:listPipelineParametersForExecution",
        "sagemaker:listPipelines",
        "sagemaker:listProcessingJobs",
        "sagemaker:listProjects",
        "sagemaker:listSpaces",
        "sagemaker:listStageDevices",
        "sagemaker:listStudioLifecycleConfigs",
        "sagemaker:listSubscribedWorkteams",
        "sagemaker:listTags",
        "sagemaker:listTrainingJobs",
        "sagemaker:listTrainingJobsForHyperParameterTuningJob",
        "sagemaker:listTransformJobs",
        "sagemaker:listTrialComponents",
        "sagemaker:listTrials",
        "sagemaker:listUserProfiles",
        "sagemaker:listWorkforces",
        "sagemaker:listWorkteams",
        "savingsplans:describeSavingsPlans",
        "scheduler:getSchedule",
        "scheduler:getScheduleGroup",
        "scheduler:listScheduleGroups",
        "scheduler:listSchedules",
        "schemas:describeCodeBinding",
        "schemas:describeDiscoverer",
        "schemas:describeRegistry",
        "schemas:describeSchema",
        "schemas:getCodeBindingSource",
        "schemas:getDiscoveredSchema",
        "schemas:getResourcePolicy",
        "schemas:listDiscoverers",
        "schemas:listRegistries",
        "schemas:listSchemas",
        "schemas:listSchemaVersions",
        "sdb:domainMetadata",
        "sdb:listDomains",
        "secretsmanager:describeSecret",
        "secretsmanager:getResourcePolicy",
        "secretsmanager:listSecrets",
        "secretsmanager:listSecretVersionIds",
        "securityhub:getEnabledStandards",
        "securityhub:getFindings",
```

```
        "securityhub:getInsightResults",
        "securityhub:getInsights",
        "securityhub:getMasterAccount",
        "securityhub:getMembers",
        "securityhub:listEnabledProductsForImport",
        "securityhub:listInvitations",
        "securityhub:listMembers",
        "securitylake:getDataLakeExceptionSubscription",
        "securitylake:getDataLakeOrganizationConfiguration",
        "securitylake:getDataLakeSources",
        "securitylake:getSubscriber",
        "securitylake:listDataLakeExceptions",
        "securitylake:listDataLakes",
        "securitylake:listLogSources",
        "securitylake:listSubscribers",
        "serverlessrepo:getApplication",
        "serverlessrepo:getApplicationPolicy",
        "serverlessrepo:getCloudFormationTemplate",
        "serverlessrepo:listApplicationDependencies",
        "serverlessrepo:listApplications",
        "serverlessrepo:listApplicationVersions",
        "servicecatalog:describeConstraint",
        "servicecatalog:describePortfolio",
        "servicecatalog:describeProduct",
        "servicecatalog:describeProductAsAdmin",
        "servicecatalog:describeProductView",
        "servicecatalog:describeProvisioningArtifact",
        "servicecatalog:describeProvisioningParameters",
        "servicecatalog:describeRecord",
        "servicecatalog:listAcceptedPortfolioShares",
        "servicecatalog:listConstraintsForPortfolio",
        "servicecatalog:listLaunchPaths",
        "servicecatalog:listPortfolioAccess",
        "servicecatalog:listPortfolios",
        "servicecatalog:listPortfoliosForProduct",
        "servicecatalog:listPrincipalsForPortfolio",
        "servicecatalog:listProvisioningArtifacts",
        "servicecatalog:listRecordHistory",
        "servicecatalog:scanProvisionedProducts",
        "servicecatalog:searchProducts",
        "servicequotas:getAssociationForServiceQuotaTemplate",
        "servicequotas:getAWSDefaultServiceQuota",
        "servicequotas:getRequestedServiceQuotaChange",
        "servicequotas:getServiceQuota",
```

```
        "servicequotas:getServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:listAWSDefaultServiceQuotas",
        "servicequotas:listRequestedServiceQuotaChangeHistory",
        "servicequotas:listRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:listServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:listServiceQuotas",
        "servicequotas:listServices",
        "ses:describeActiveReceiptRuleSet",
        "ses:describeConfigurationSet",
        "ses:describeReceiptRule",
        "ses:describeReceiptRuleSet",
        "ses:getAccount",
        "ses:getAccountSendingEnabled",
        "ses:getBlacklistReports",
        "ses:getConfigurationSet",
        "ses:getConfigurationSetEventDestinations",
        "ses:getContactList",
        "ses:getDedicatedIp",
        "ses:getDedicatedIpPool",
        "ses:getDedicatedIps",
        "ses:getDeliverabilityDashboardOptions",
        "ses:getDeliverabilityTestReport",
        "ses:getDomainDeliverabilityCampaign",
        "ses:getDomainStatisticsReport",
        "ses:getEmailIdentity",
        "ses:getIdentityDkimAttributes",
        "ses:getIdentityMailFromDomainAttributes",
        "ses:getIdentityNotificationAttributes",
        "ses:getIdentityPolicies",
        "ses:getIdentityVerificationAttributes",
        "ses:getImportJob",
        "ses:getSendQuota",
        "ses:getSendStatistics",
        "ses:listConfigurationSets",
        "ses:listContactLists",
        "ses:listContacts",
        "ses:listCustomVerificationEmailTemplates",
        "ses:listDedicatedIpPools",
        "ses:listDeliverabilityTestReports",
        "ses:listDomainDeliverabilityCampaigns",
        "ses:listEmailIdentities",
        "ses:listEmailTemplates",
        "ses:listIdentities",
        "ses:listIdentityPolicies",
```

```
        "ses:listImportJobs",
        "ses:listReceiptFilters",
        "ses:listReceiptRuleSets",
        "ses:listRecommendations",
        "ses:listTagsForResource",
        "ses:listTemplates",
        "ses:listVerifiedEmailAddresses",
        "shield:describeAttack",
        "shield:describeProtection",
        "shield:describeSubscription",
        "shield:listAttacks",
        "shield:listProtections",
        "sms-voice:getConfigurationSetEventDestinations",
        "sms:getConnectors",
        "sms:getReplicationJobs",
        "sms:getReplicationRuns",
        "sms:getServers",
        "snowball:describeAddress",
        "snowball:describeAddresses",
        "snowball:describeJob",
        "snowball:getSnowballUsage",
        "snowball:listJobs",
        "snowball:listServiceVersions",
        "sns:checkIfPhoneNumberIsOptedOut",
        "sns:getDataProtectionPolicy",
        "sns:getEndpointAttributes",
        "sns:getPlatformApplicationAttributes",
        "sns:getSMSAttributes",
        "sns:getSMSSandboxAccountStatus",
        "sns:getSubscriptionAttributes",
        "sns:getTopicAttributes",
        "sns:listEndpointsByPlatformApplication",
        "sns:listOriginationNumbers",
        "sns:listPhoneNumbersOptedOut",
        "sns:listPlatformApplications",
        "sns:listSMSSandboxPhoneNumbers",
        "sns:listSubscriptions",
        "sns:listSubscriptionsByTopic",
        "sns:listTopics",
        "sqs:getQueueAttributes",
        "sqs:getQueueUrl",
        "sqs:listDeadLetterSourceQueues",
        "sqs:listQueues",
        "ssm-contacts:describeEngagement",
```

```
        "ssm-contacts:describePage",
        "ssm-contacts:getContact",
        "ssm-contacts:getContactChannel",
        "ssm-contacts:getContactPolicy",
        "ssm-contacts:getRotation",
        "ssm-contacts:getRotationOverride",
        "ssm-contacts:listContactChannels",
        "ssm-contacts:listContacts",
        "ssm-contacts:listEngagements",
        "ssm-contacts:listPageReceipts",
        "ssm-contacts:listPageResolutions",
        "ssm-contacts:listPagesByContact",
        "ssm-contacts:listPagesByEngagement",
        "ssm-contacts:listPreviewRotationShifts",
        "ssm-contacts:listRotationOverrides",
        "ssm-contacts:listRotations",
        "ssm-contacts:listRotationShifts",
        "ssm-incidents:getIncidentRecord",
        "ssm-incidents:getReplicationSet",
        "ssm-incidents:getResourcePolicies",
        "ssm-incidents:getResponsePlan",
        "ssm-incidents:getTimelineEvent",
        "ssm-incidents:listIncidentRecords",
        "ssm-incidents:listRelatedItems",
        "ssm-incidents:listReplicationSets",
        "ssm-incidents:listResponsePlans",
        "ssm-incidents:listTimelineEvents",
        "ssm-sap:getApplication",
        "ssm-sap:getComponent",
        "ssm-sap:getDatabase",
        "ssm-sap:getOperation",
        "ssm-sap:getResourcePermission",
        "ssm-sap:listApplications",
        "ssm-sap:listComponents",
        "ssm-sap:listDatabases",
        "ssm-sap:listOperations",
        "ssm:describeActivations",
        "ssm:describeAssociation",
        "ssm:describeAssociationExecutions",
        "ssm:describeAssociationExecutionTargets",
        "ssm:describeAutomationExecutions",
        "ssm:describeAutomationStepExecutions",
        "ssm:describeAvailablePatches",
        "ssm:describeDocument",
```

```
        "ssm:describeDocumentPermission",
        "ssm:describeEffectiveInstanceAssociations",
        "ssm:describeEffectivePatchesForPatchBaseline",
        "ssm:describeInstanceAssociationsStatus",
        "ssm:describeInstanceInformation",
        "ssm:describeInstancePatches",
        "ssm:describeInstancePatchStates",
        "ssm:describeInstancePatchStatesForPatchGroup",
        "ssm:describeInventoryDeletions",
        "ssm:describeMaintenanceWindowExecutions",
        "ssm:describeMaintenanceWindowExecutionTaskInvocations",
        "ssm:describeMaintenanceWindowExecutionTasks",
        "ssm:describeMaintenanceWindows",
        "ssm:describeMaintenanceWindowSchedule",
        "ssm:describeMaintenanceWindowsForTarget",
        "ssm:describeMaintenanceWindowTargets",
        "ssm:describeMaintenanceWindowTasks",
        "ssm:describeOpsItems",
        "ssm:describeParameters",
        "ssm:describePatchBaselines",
        "ssm:describePatchGroups",
        "ssm:describePatchGroupState",
        "ssm:describePatchProperties",
        "ssm:describeSessions",
        "ssm:getAutomationExecution",
        "ssm:getCalendarState",
        "ssm:getCommandInvocation",
        "ssm:getConnectionStatus",
        "ssm:getDefaultPatchBaseline",
        "ssm:getDeployablePatchSnapshotForInstance",
        "ssm:getInventorySchema",
        "ssm:getMaintenanceWindow",
        "ssm:getMaintenanceWindowExecution",
        "ssm:getMaintenanceWindowExecutionTask",
        "ssm:getMaintenanceWindowExecutionTaskInvocation",
        "ssm:getMaintenanceWindowTask",
        "ssm:getOpsItem",
        "ssm:getOpsMetadata",
        "ssm:getOpsSummary",
        "ssm:getPatchBaseline",
        "ssm:getPatchBaselineForPatchGroup",
        "ssm:getResourcePolicies",
        "ssm:getServiceSetting",
        "ssm:listAssociations",
```

```
        "ssm:listAssociationVersions",
        "ssm:listCommandInvocations",
        "ssm:listCommands",
        "ssm:listComplianceItems",
        "ssm:listComplianceSummaries",
        "ssm:listDocuments",
        "ssm:listDocumentMetadataHistory",
        "ssm:listDocumentVersions",
        "ssm:listOpsItemEvents",
        "ssm:listOpsItemRelatedItems",
        "ssm:listOpsMetadata",
        "ssm:listResourceComplianceSummaries",
        "ssm:listResourceDataSync",
        "ssm:listTagsForResource",
        "sso:describeApplicationAssignment",
        "sso:describeApplicationProvider",
        "sso:describeApplication",
        "sso:describeInstance",
        "sso:describeTrustedTokenIssuer",
        "sso:getApplicationAccessScope",
        "sso:getApplicationAssignmentConfiguration",
        "sso:getApplicationAuthenticationMethod",
        "sso:getApplicationGrant",
        "sso:getApplicationInstance",
        "sso:getApplicationTemplate",
        "sso:getManagedApplicationInstance",
        "sso:getSharedSsoConfiguration",
        "sso:listApplicationAccessScopes",
        "sso:listApplicationAssignments",
        "sso:listApplicationAuthenticationMethods",
        "sso:listApplicationGrants",
        "sso:listApplicationInstances",
        "sso:listApplicationProviders",
        "sso:listApplications",
        "sso:listApplicationTemplates",
        "sso:listDirectoryAssociations",
        "sso:listInstances",
        "sso:listProfileAssociations",
        "sso:listTrustedTokenIssuers",
        "states:describeActivity",
        "states:describeExecution",
        "states:describeMapRun",
        "states:describeStateMachine",
        "states:describeStateMachineAlias",
```

```
        "states:describeStateMachineForExecution",
        "states:getExecutionHistory",
        "states:listActivities",
        "states:listExecutions",
        "states:listMapRuns",
        "states:listStateMachineAliases",
        "states:listStateMachines",
        "states:listStateMachineVersions",
        "storagegateway:describeBandwidthRateLimit",
        "storagegateway:describeCache",
        "storagegateway:describeCachediSCSIVolumes",
        "storagegateway:describeFileSystemAssociations",
        "storagegateway:describeGatewayInformation",
        "storagegateway:describeMaintenanceStartTime",
        "storagegateway:describeNFSFileShares",
        "storagegateway:describeSMBFileShares",
        "storagegateway:describeSMBSettings",
        "storagegateway:describeSnapshotSchedule",
        "storagegateway:describeStorediSCSIVolumes",
        "storagegateway:describeTapeArchives",
        "storagegateway:describeTapeRecoveryPoints",
        "storagegateway:describeTapes",
        "storagegateway:describeUploadBuffer",
        "storagegateway:describeVTLDevices",
        "storagegateway:describeWorkingStorage",
        "storagegateway:listAutomaticTapeCreationPolicies",
        "storagegateway:listFileShares",
        "storagegateway:listFileSystemAssociations",
        "storagegateway:listGateways",
        "storagegateway:listLocalDisks",
        "storagegateway:listTagsForResource",
        "storagegateway:listTapes",
        "storagegateway:listVolumeInitiators",
        "storagegateway:listVolumeRecoveryPoints",
        "storagegateway:listVolumes",
        "swf:countClosedWorkflowExecutions",
        "swf:countOpenWorkflowExecutions",
        "swf:countPendingActivityTasks",
        "swf:countPendingDecisionTasks",
        "swf:describeActivityType",
        "swf:describeDomain",
        "swf:describeWorkflowExecution",
        "swf:describeWorkflowType",
        "swf:getWorkflowExecutionHistory",
```

```
        "swf:listActivityTypes",
        "swf:listClosedWorkflowExecutions",
        "swf:listDomains",
        "swf:listOpenWorkflowExecutions",
        "swf:listWorkflowTypes",
        "synthetics:describeCanaries",
        "synthetics:describeCanariesLastRun",
        "synthetics:describeRuntimeVersions",
        "synthetics:getCanary",
        "synthetics:getCanaryRuns",
        "synthetics:getGroup",
        "synthetics:listAssociatedGroups",
        "synthetics:listGroupResources",
        "synthetics:listGroups",
        "tiros:createQuery",
        "tiros:getQueryAnswer",
        "tiros:getQueryExplanation",
        "transcribe:describeLanguageModel",
        "transcribe:getCallAnalyticsCategory",
        "transcribe:getCallAnalyticsJob",
        "transcribe:getMedicalTranscriptionJob",
        "transcribe:getMedicalVocabulary",
        "transcribe:getTranscriptionJob",
        "transcribe:getVocabulary",
        "transcribe:getVocabularyFilter",
        "transcribe:listCallAnalyticsCategories",
        "transcribe:listCallAnalyticsJobs",
        "transcribe:listLanguageModels",
        "transcribe:listMedicalTranscriptionJobs",
        "transcribe:listMedicalVocabularies",
        "transcribe:listTranscriptionJobs",
        "transcribe:listVocabularies",
        "transcribe:listVocabularyFilters",
        "transfer:describeAccess",
        "transfer:describeAgreement",
        "transfer:describeConnector",
        "transfer:describeExecution",
        "transfer:describeProfile",
        "transfer:describeServer",
        "transfer:describeUser",
        "transfer:describeWorkflow",
        "transfer:listAccesses",
        "transfer:listAgreements",
        "transfer:listConnectors",
```

```
        "transfer:listExecutions",
        "transfer:listHostKeys",
        "transfer:listProfiles",
        "transfer:listServers",
        "transfer:listTagsForResource",
        "transfer:listUsers",
        "transfer:listWorkflows",
        "transfer:sendWorkflowStepState",
        "trustedadvisor:getOrganizationRecommendation",
        "trustedadvisor:getRecommendation",
        "trustedadvisor:listChecks",
        "trustedadvisor:listOrganizationRecommendationAccounts",
        "trustedadvisor:listOrganizationRecommendationResources",
        "trustedadvisor:listOrganizationRecommendations",
        "trustedadvisor:listRecommendationResources",
        "trustedadvisor:listRecommendations",
        "verifiedpermissions:getIdentitySource",
        "verifiedpermissions:getPolicy",
        "verifiedpermissions:getPolicyStore",
        "verifiedpermissions:getPolicyTemplate",
        "verifiedpermissions:getSchema",
        "verifiedpermissions:listIdentitySources",
        "verifiedpermissions:listPolicies",
        "verifiedpermissions:listPolicyStores",
        "verifiedpermissions:listPolicyTemplates",
        "vpc-lattice:getAccessLogSubscription",
        "vpc-lattice:getAuthPolicy",
        "vpc-lattice:getListener",
        "vpc-lattice:getResourcePolicy",
        "vpc-lattice:getRule",
        "vpc-lattice:getService",
        "vpc-lattice:getServiceNetwork",
        "vpc-lattice:getServiceNetworkServiceAssociation",
        "vpc-lattice:getServiceNetworkVpcAssociation",
        "vpc-lattice:getTargetGroup",
        "vpc-lattice:listAccessLogSubscriptions",
        "vpc-lattice:listListeners",
        "vpc-lattice:listRules",
        "vpc-lattice:listServiceNetworks",
        "vpc-lattice:listServiceNetworkServiceAssociations",
        "vpc-lattice:listServiceNetworkVpcAssociations",
        "vpc-lattice:listServices",
        "vpc-lattice:listTargetGroups",
        "vpc-lattice:listTargets",
```

```
        "waf-regional:getByteMatchSet",
        "waf-regional:getChangeTokenStatus",
        "waf-regional:getGeoMatchSet",
        "waf-regional:getIPSet",
        "waf-regional:getLoggingConfiguration",
        "waf-regional:getRateBasedRule",
        "waf-regional:getRegexMatchSet",
        "waf-regional:getRegexPatternSet",
        "waf-regional:getRule",
        "waf-regional:getRuleGroup",
        "waf-regional:getSqlInjectionMatchSet",
        "waf-regional:getWebACL",
        "waf-regional:getWebACLForResource",
        "waf-regional:listActivatedRulesInRuleGroup",
        "waf-regional:listByteMatchSets",
        "waf-regional:listGeoMatchSets",
        "waf-regional:listIPSets",
        "waf-regional:listLoggingConfigurations",
        "waf-regional:listRateBasedRules",
        "waf-regional:listRegexMatchSets",
        "waf-regional:listRegexPatternSets",
        "waf-regional:listResourcesForWebACL",
        "waf-regional:listRuleGroups",
        "waf-regional:listRules",
        "waf-regional:listSqlInjectionMatchSets",
        "waf-regional:listWebACLs",
        "waf:getByteMatchSet",
        "waf:getChangeTokenStatus",
        "waf:getGeoMatchSet",
        "waf:getIPSet",
        "waf:getLoggingConfiguration",
        "waf:getRateBasedRule",
        "waf:getRegexMatchSet",
        "waf:getRegexPatternSet",
        "waf:getRule",
        "waf:getRuleGroup",
        "waf:getSampledRequests",
        "waf:getSizeConstraintSet",
        "waf:getSqlInjectionMatchSet",
        "waf:getWebACL",
        "waf:getXssMatchSet",
        "waf:listActivatedRulesInRuleGroup",
        "waf:listByteMatchSets",
        "waf:listGeoMatchSets",
```

```
        "waf:listIPSets",
        "waf:listLoggingConfigurations",
        "waf:listRateBasedRules",
        "waf:listRegexMatchSets",
        "waf:listRegexPatternSets",
        "waf:listRuleGroups",
        "waf:listRules",
        "waf:listSizeConstraintSets",
        "waf:listSqlInjectionMatchSets",
        "waf:listWebACLs",
        "waf:listXssMatchSets",
        "wafv2:checkCapacity",
        "wafv2:describeManagedRuleGroup",
        "wafv2:getIPSet",
        "wafv2:getLoggingConfiguration",
        "wafv2:getPermissionPolicy",
        "wafv2:getRateBasedStatementManagedKeys",
        "wafv2:getRegexPatternSet",
        "wafv2:getRuleGroup",
        "wafv2:getSampledRequests",
        "wafv2:getWebACL",
        "wafv2:getWebACLForResource",
        "wafv2:listAvailableManagedRuleGroups",
        "wafv2:listIPSets",
        "wafv2:listLoggingConfigurations",
        "wafv2:listRegexPatternSets",
        "wafv2:listResourcesForWebACL",
        "wafv2:listRuleGroups",
        "wafv2:listTagsForResource",
        "wafv2:listWebACLs",
        "workdocs:checkAlias",
        "workdocs:describeAvailableDirectories",
        "workdocs:describeInstances",
        "workmail:describeGroup",
        "workmail:describeOrganization",
        "workmail:describeResource",
        "workmail:describeUser",
        "workmail:listAliases",
        "workmail:listGroupMembers",
        "workmail:listGroups",
        "workmail:listMailboxPermissions",
        "workmail:listOrganizations",
        "workmail:listResourceDelegates",
        "workmail:listResources",
```

```
        "workmail:listUsers",
        "workspaces-web:getBrowserSettings",
        "workspaces-web:getIdentityProvider",
        "workspaces-web:getNetworkSettings",
        "workspaces-web:getPortal",
        "workspaces-web:getPortalServiceProviderMetadata",
        "workspaces-web:getTrustStoreCertificate",
        "workspaces-web:getUserSettings",
        "workspaces-web:listBrowserSettings",
        "workspaces-web:listIdentityProviders",
        "workspaces-web:listNetworkSettings",
        "workspaces-web:listPortals",
        "workspaces-web:listTagsForResource",
        "workspaces-web:listTrustStoreCertificates",
        "workspaces-web:listTrustStores",
        "workspaces-web:listUserSettings",
        "workspaces:describeAccount",
        "workspaces:describeAccountModifications",
        "workspaces:describeIpGroups",
        "workspaces:describeTags",
        "workspaces:describeWorkspaceBundles",
        "workspaces:describeWorkspaceDirectories",
        "workspaces:describeWorkspaceImages",
        "workspaces:describeWorkspaces",
        "workspaces:describeWorkspacesConnectionStatus"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSSystemsManagerAccountDiscoveryServicePolicy

`AWSSystemsManagerAccountDiscoveryServicePolicy`adalah kebijakanAWS terkelola yang: Izin HibahAWS Systems Manager (SSM) untuk menemukanAkun AWS informasi.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan tidak dapat dilampirkan pada pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 Oktober 2019, 17:21 UTC
- Waktu yang telah diedit: 17 Oktober 2022, 20.25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
```

```
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSSystemsManagerChangeManagementServicePolicy

`AWSSystemsManagerChangeManagementServicePolicy`adalah kebijakanAWS terkelola yang: Menyediakan akses keAWS sumber daya yang dikelola atau digunakan oleh kerangka manajemen perubahanAWS Systems Manager.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini untuk pengguna, peran Anda.

Kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 Desember 2020, 22:21 UTC
- Waktu yang telah diedit: 07 Desember 2020, 22.21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Kebijakan ini adalah versi yang menentukan izin untuk kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation",
        "ssm:CreateOpsItem",
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:GetAutomationExecution",
        "ssm:GetCalendarState",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:IsMemberInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSSystemsManagerForSAPFullAccess

`AWSSystemsManagerForSAPFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS Systems Manager untuk layanan SAP

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSSystemsManagerForSAPFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 17 November 2022, 02:11 UTC
- Waktu yang telah diedit: 18 November 2022, 21.58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm-sap.amazonaws.com/
AWSServiceRoleForAWSSSMForSAP"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm-sap.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSSystemsManagerForSAPReadOnlyAccess

`AWSSystemsManagerForSAPReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja keAWS Systems Manager untuk layanan SAP

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSSystemsManagerForSAPReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 17 November 2022, 02:11 UTC

- Waktu yang telah diedit: 17 November 2022, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",
        "ssm-sap:list*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSSystemsManagerOpsDataSyncServiceRolePolicy

`AWSSystemsManagerOpsDataSyncServiceRolePolicy`adalah kebijakan AWS terkelola yang: Peran IAM untuk SSM Explorer untuk mengelola OpsData operasi terkait

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 April 2021, 20:42 UTC
- Waktu yang telah diedit: 28 Juni 2023, 22.53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ExplorerSecurityHubOpsItem" : "true"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "securityhub:GetFindings",
        "securityhub:BatchUpdateFindings"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "securityhub:ASFFSyntaxPath/Workflow.Status" : "SUPPRESSED"
        }
      }
```

```
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Confidence" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Criticality" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Note.Text" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Note.UpdatedBy" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/RelatedFindings" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Types" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/UserDefinedFields.key" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/UserDefinedFields.value" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/VerificationState" : false
```

```
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSThinkboxAssetServerPolicy

`AWSThinkboxAssetServerPolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memberi Server AsetAWS Portal izin yang diperlukan untuk operasi normal.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSThinkboxAssetServerPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:18 Mei 2020
- Waktu yang telah diedit: 27 Mei 2020, 19.18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSThinkboxAWSPortalAdminPolicy

`AWSThinkboxAWSPortalAdminPolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan perangkat lunak Tenggat Waktu AWS Thinkbox akses penuh ke beberapa AWS layanan seperti yang diperlukan untuk administrasi Portal. AWS Ini termasuk akses untuk membuat tag arbitrer pada beberapa jenis sumber daya EC2.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSThinkboxAWSPortalAdminPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:41 UTC
- Waktu telah diedit: 23 Februari 2024, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxAWSPortal1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
```

```
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAddresses",
        "ec2:DescribeFleets",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNatGateways",
        "ec2:DescribeTags",
        "ec2:DescribeKeyPairs",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRegions",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:GetConsoleOutput",
        "ec2:ImportKeyPair",
        "ec2:ReleaseAddress",
        "ec2:RequestSpotFleet",
        "ec2:CancelSpotFleetRequests",
        "ec2:DisassociateAddress",
        "ec2:DeleteFleets",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteVpc",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteRoute",
```

```
        "ec2:DeleteRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DeleteNatGateway",
        "ec2:DetachInternetGateway",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyFleet",
        "ec2:ModifySpotFleetRequest",
        "ec2:ModifyVpcAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal2",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal3",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/AWSPortal*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal4",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ReverseForwarder"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal5",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal6",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:PlacementGroup" : "*DeadlinePlacementGroup*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:PlacementGroup" : "*DeadlinePlacementGroup*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal8",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal10",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal11",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AWSPortal*"
```

```
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal12",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicyVersions"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/AWSPortal*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal13",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPortal*",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal14",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPortal*",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "cloudformation.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal15",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal16",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketVersioning",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:PutBucketLogging",
        "s3:PutBucketTagging",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObjectVersion"
      ],
```

```
      "Resource" : [
        "arn:aws:s3::*:awsportal*",
        "arn:aws:s3::*:stack*",
        "arn:aws:s3::*:aws-portal-cache*",
        "arn:aws:s3::*:logs-for-aws-portal-cache*",
        "arn:aws:s3::*:logs-for-stack*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal17",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3::*:logs-for-aws-portal-cache*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal18",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketOwnershipControls"
      ],
      "Resource" : [
        "arn:aws:s3::*:logs-for-stack*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal19",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal20",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
    },
```

```
    {
      "Sid" : "AWSThinkboxAWSPortal21",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListStackResources",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateTerminationProtection"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/stack*/*",
        "arn:aws:cloudformation:*:*:stack/Deadline*/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal22",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:EstimateTemplateCost",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal23",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DeleteRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/thinkbox*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal24",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal25",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal26",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : [
            "rcs-tls-pw*"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal27",
      "Effect" : "Allow",
      "Action" : [
```

```
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSThinkboxAWSPortalGatewayPolicy

`AWSThinkboxAWSPortalGatewayPolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memberi mesinAWS Portal Gateway izin yang diperlukan untuk operasi normal.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSThinkboxAWSPortalGatewayPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:05 UTC
- Waktu yang telah diedit: 30 Juni 2020, 16.02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "dynamodb:Scan",
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*/gateway_certs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw-stack*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSThinkboxAWSPortalWorkerPolicy

`AWSThinkboxAWSPortalWorkerPolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan kepada Pekerja Batas Waktu diAWS Portal izin yang diperlukan untuk operasi normal.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSThinkboxAWSPortalWorkerPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:15 UTC
- Waktu yang telah diedit: 07 Desember 2020, 23.27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineRole" : "DeadlineRenderNode"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*/gateway_certs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWS*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSThinkboxDeadlineResourceTrackerAccessPolicy

`AWSThinkboxDeadlineResourceTrackerAccessPolicy`adalah kebijakanAWS terkelola yang: Memberikan izin yang diperlukan untuk pengoperasian Pelacak Sumber Daya Tenggat WaktuAWS Thinkbox. Ini termasuk akses penuh ke beberapa tindakan EC2, termasuk DeleteFleets dan CancelSpotFleetRequests.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSThinkboxDeadlineResourceTrackerAccessPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Mei 2020
- Waktu yang telah diedit: 27 Mei 2020, 19.25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchWriteItem",
        "dynamodb:DeleteItem",
```

```
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:PutItem",
        "dynamodb:Scan",
        "dynamodb:UpdateItem",
        "dynamodb:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelSpotFleetRequests",
        "ec2:DeleteFleets",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeFleets",
        "ec2:DescribeInstances",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/DeadlineTrackedAWSResource" : "*"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutEvents"
      ],
      "Resource" : [
        "arn:aws:events:*:*:event-bus/default"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
```

```
        "sqs:ReceiveMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeStateMessageQueue*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSThinkboxDeadlineResourceTrackerAdminPolicy

`AWSThinkboxDeadlineResourceTrackerAdminPolicy`adalah kebijakanAWS terkelola yang: Memberikan izin yang diperlukan untuk membuat, menghancurkan, dan mengelola Pelacak Sumber Daya Tenggat WaktuAWS Thinkbox.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSThinkboxDeadlineResourceTrackerAdminPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:29 UTC
- Waktu yang telah diedit: 22 Juni 2022, 18.08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
```

```
        "cloudformation:UpdateTerminationProtection"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable",
        "dynamodb:ListTagsOfResource",
        "dynamodb:TagResource",
        "dynamodb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchWriteItem",
        "dynamodb:Scan"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DeadlineResourceTracker*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTrackerAccess*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/dynamodb.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_DynamoDBTable"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
```

```
        "StringLike" : {
          "lambda:FunctionArn" : [
            "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ],
      "Condition" : {
        "StringLike" : {
          "lambda:Principal" : "events.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:DeleteFunctionConcurrency",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "lambda:PutFunctionConcurrency",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/deadline_aws_resource_tracker-*.zip",
        "arn:aws:s3:::*/DeadlineAWSResourceTrackerTemplate-*.yaml"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:TagQueue",
        "sqs:UntagQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*",
        "arn:aws:sqs:*:*:DeadlineResourceTracker*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

`AWSThinkboxDeadlineSpotEventPluginAdminPolicy`adalah kebijakanAWS terkelola yang: Memberikan izin yang diperlukan untuk Plugin Acara Titik Batas WaktuAWS Thinkbox. Ini termasuk izin untuk meminta, memodifikasi, dan membatalkan armada spot, serta PassRole izin terbatas.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSThinkboxDeadlineSpotEventPluginAdminPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:38 UTC
- Waktu yang telah diedit: 27 Mei 2020, 19.38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelSpotFleetRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:RequestSpotFleet"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role",
```

```
        "arn:aws:iam::*:role/DeadlineSpot*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

`AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`adalah kebijakanAWS terkelola yang: Hibah izin yang diperlukan untuk instans EC2 yang menjalankan perangkat lunakAWS Thinkbox Deadline Spot Event Plugin Worker.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSThinkboxDeadlineSpotEventPluginWorkerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Mei 2020, 19:35 UTC
- Waktu yang telah diedit: 07 Desember 2020 23.31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineTrackedAWSResource" : "SpotEventPlugin"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineResourceTracker" : "SpotEventPlugin"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueUrl",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSTransferConsoleFullAccess

`AWSTransferConsoleFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS Transfer melaluiAWS Management Console

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSTransferConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 14 Desember 2020, 19:33 UTC
- Waktu yang telah diedit: 14 Desember 2020 19.33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "transfer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "health:DescribeEventAggregates",
        "iam:GetPolicyVersion",
        "iam:ListPolicies",
```

```
        "iam:ListRoles",
        "route53:ListHostedZones",
        "s3:ListAllMyBuckets",
        "transfer:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSTransferFullAccess

`AWSTransferFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke LayananAWS Transfer.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSTransferFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 14 Desember 2020, 19:37 UTC
- Waktu yang telah diedit: 14 Desember 2020 19.37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "transfer:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "transfer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSTransferLoggingAccess

`AWSTransferLoggingAccess`adalah kebijakanAWS terkelola yang: MemungkinkanAWS Transfer akses penuh untuk membuat aliran log dan grup dan menempatkan peristiwa log ke akun Anda

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSTransferLoggingAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Januari 2019, 15:32 UTC
- Waktu yang telah diedit: 14 Januari 2019 15.32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSTransferReadOnlyAccess

`AWSTransferReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses readonly ke layananAWS Transfer.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSTransferReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Agustus 2020, 17:54 UTC
- Waktu yang telah diedit: 27 Agustus 2020 17.54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSTrustedAdvisorPriorityFullAccess

`AWSTrustedAdvisorPriorityFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke PrioritasAWS Trusted Advisor. Kebijakan ini juga memungkinkan pengguna untuk menambahkan Trusted Advisor sebagai layanan tepercaya denganAWS Organizations dan untuk menentukan akun administrator yang didelegasikan untuk Prioritas Trusted Advisor.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSTrustedAdvisorPriorityFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 16 Agustus 2022, 16:08 UTC
- Waktu yang telah diedit: 16 Agustus 2022, 16.08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeAccount*",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:DownloadRisk",
        "trustedadvisor:UpdateRiskStatus",
        "trustedadvisor:DescribeNotificationConfigurations",
        "trustedadvisor:UpdateNotificationConfigurations",
        "trustedadvisor:DeleteNotificationConfigurationForDelegatedAdmin",
        "trustedadvisor:SetOrganizationAccess"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
```

```
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "reporting.trustedadvisor.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSTrustedAdvisorPriorityReadOnlyAccess

`AWSTrustedAdvisorPriorityReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke PrioritasAWS Trusted Advisor. Ini termasuk izin untuk melihat akun administrator yang didelegasikan.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSTrustedAdvisorPriorityReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 16 Agustus 2022, 16:35 UTC
- Waktu yang telah diedit: 16 Agustus 2022, 16.35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeAccount*",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:DownloadRisk",
        "trustedadvisor:DescribeNotificationConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSTrustedAdvisorReportingServiceRolePolicy

`AWSTrustedAdvisorReportingServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan Layanan untuk Pelaporan Multi-akun Trusted Advisor

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

detail kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 November 2019, 17:41 UTC
- Waktu yang telah diedit: 28 Pebruari 2023, 23.23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSTrustedAdvisorServiceRolePolicy

`AWSTrustedAdvisorServiceRolePolicy`adalah kebijakan AWS terkelola yang: Akses ke Layanan AWS Trusted Advisor untuk membantu mengurangi biaya, meningkatkan kinerja, dan meningkatkan keamanan lingkungan AndaAWS.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 22 Februari 2018, 21:24 UTC
- Waktu telah diedit: 18 Januari 2024, 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v12 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedAdvisorServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudfront:ListDistributions",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:GetMetricStatistics",
```

```
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeLaunchTemplateVersions",
        "ecs:DescribeTaskDefinition",
        "ecs:ListTaskDefinitions",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "iam:GenerateCredentialReport",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetServerCertificate",
        "iam:ListServerCertificates",
        "kinesis:DescribeLimits",
        "kafka:ListClustersV2",
        "kafka:ListNodes",
        "outposts:ListAssets",
        "outposts:GetOutpost",
        "outposts:ListOutposts",
        "rds:DescribeAccountAttributes",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
```

```
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroupOptions",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribeReservedDBInstances",
        "rds:DescribeReservedDBInstancesOfferings",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeReservedNodeOfferings",
        "redshift:DescribeReservedNodes",
        "route53:GetAccountLimit",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetLifecycleConfiguration",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "ses:GetSendQuota",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin dengan hak istimewa paling sedikit

AWSUserNotificationsServiceLinkedRolePolicy

`AWSUserNotificationsServiceLinkedRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan PemberitahuanAWS Pengguna untuk memanggilAWS layanan atas nama Anda.

Menggunakan

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan

detail

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 19 April 2023, 13:28 UTC
- Waktu yang telah diedit: 19 April 2023, 13.28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:ListTargetsByRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AWSUserNotificationsManagedRule-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Notifications"
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSVendorInsightsAssessorFullAccess

`AWSVendorInsightsAssessorFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh untuk melihat sumber daya Vendor Insights berjudul dan mengelola langganan Vendor Insights

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSVendorInsightsAssessorFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 26 Juli 2022, 15:05 UTC
- Waktu yang telah diedit: 01 Desember 2022, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetProfileAccessTerms",
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreateAgreementRequest",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:AcceptAgreementRequest",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:CancelAgreement"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:AgreementType" : "VendorInsightsAgreement"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSVendorInsightsAssessorReadOnly

`AWSVendorInsightsAssessorReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca untuk melihat sumber daya Vendor Insights berjudul

Menggunakan kebijakan

Anda dapat melampirkan`AWSVendorInsightsAssessorReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 26 Juli 2022, 15:05 UTC
- Waktu yang telah diedit: 01 Desember 2022, 00.55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSVendorInsightsVendorFullAccess

`AWSVendorInsightsVendorFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh untuk membuat dan mengelola sumber daya Vendor Insights

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSVendorInsightsVendorFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 26 Juli 2022, 15:05 UTC
- Waktu telah diedit: 19 Oktober 2023, 01:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:DescribeEntity",
      "Resource" : "arn:aws:aws-marketplace:*:*:*/SaaSProduct/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:ListEntities",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:CreateDataSource",
        "vendor-insights:UpdateDataSource",
        "vendor-insights:DeleteDataSource",
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:CreateSecurityProfile",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:AssociateDataSource",
        "vendor-insights:DisassociateDataSource",
        "vendor-insights:UpdateSecurityProfile",
        "vendor-insights:ActivateSecurityProfile",
        "vendor-insights:DeactivateSecurityProfile",
        "vendor-insights:UpdateSecurityProfileSnapshotCreationConfiguration",
        "vendor-insights:UpdateSecurityProfileSnapshotReleaseConfiguration",
        "vendor-insights:ListSecurityProfileSnapshots",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:TagResource",
        "vendor-insights:UntagResource",
        "vendor-insights:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:GetAgreementApprovalRequest",
```

```
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:CancelAgreement",
        "aws-marketplace:SearchAgreements"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:AgreementType" : "VendorInsightsAgreement"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSVendorInsightsVendorReadOnly

`AWSVendorInsightsVendorReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca untuk melihat sumber daya Vendor Insights

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSVendorInsightsVendorReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 26 Juli 2022, 15:05 UTC
- Waktu yang telah diedit: 01 Desember 2022, 00:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:DescribeEntity",
      "Resource" : "arn:aws:aws-marketplace:*:*:*/SaaSProduct/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:ListEntities",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots",
        "vendor-insights:ListTagsForResource"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSVpcLatticeServiceRolePolicy

`AWSVpcLatticeServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan VPC Lattice mengaksesAWS sumber daya atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 30 November 2022, 20:47 UTC

- Waktu yang telah diedit: 30 November 2022, 20.47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/VpcLattice"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSVPCS2SVpnServiceRolePolicy

`AWSVPCS2SVpnServiceRolePolicy`adalah kebijakanAWS terkelola yang: Izinkan Site-to-Site VPN untuk membuat dan mengelola sumber daya yang terkait dengan Koneksi VPN Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 06 Agustus 2019, 14:13 UTC
- Waktu yang telah diedit: 06 Agustus 2019 14.13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSVPCTransitGatewayServiceRolePolicy

`AWSVPCTransitGatewayServiceRolePolicy`adalah kebijakanAWS terkelola yang: Izinkan VPC Transit Gateway untuk membuat dan mengelola sumber daya yang diperlukan untuk Lampiran VPC Transit Gateway Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 November 2018, 16:21 UTC
- Waktu yang telah diedit: 15 April 2021 16.31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AssignIpv6Addresses",
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "*",
      "Effect" : "Allow",
      "Sid" : "0"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSVPCVerifiedAccessServiceRolePolicy

`AWSVPCVerifiedAccessServiceRolePolicy`adalah kebijakan AWS terkelola yang: Kebijakan untuk mengaktifkan layanan Akses AWS Terverifikasi untuk menyediakan titik akhir atas nama Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 29 November 2022, 03:35 UTC

- Waktu telah diedit: 17 November 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VerifiedAccessRoleModifyTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VerifiedAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VerifiedAccessRoleModifyNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "VerifiedAccessRoleNetworkInterfaceActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "VerifiedAccessRoleTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/VerifiedAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VerifiedAccessRoleTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSWAFConsoleFullAccess

`AWSWAFConsoleFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke AWS WAF melalui. AWS Management Console Perhatikan bahwa kebijakan ini juga memberikan izin untuk mencantumkan dan memperbarui CloudFront distribusi Amazon, izin untuk melihat load balancer pada AWS Elastic Load Balancing, izin untuk melihat API dan tahapan REST Amazon API Gateway API, izin untuk mencantumkan dan melihat CloudWatch metrik Amazon, dan izin untuk melihat wilayah yang diaktifkan dalam akun.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSWAFConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 April 2020, 18:38 UTC
- Waktu yang telah diedit: 05 Juni 2023, 20.56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:SetWebACL",
```

```
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:UpdateDistribution",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeRegions",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:SetWebACL",
        "appsync:ListGraphqlApis",
        "appsync:SetWebACL",
        "waf-regional:*",
        "waf:*",
        "wafv2:*",
        "s3:ListAllMyBuckets",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "cognito-idp:ListUserPools",
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:ListResourcesForWebACL",
        "cognito-idp:GetWebACLForResource",
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl",
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogDeliverySubscription",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
```

```
    {
      "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
      "Action" : [
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Effect" : "Allow",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSWAFConsoleReadOnlyAccess

`AWSWAFConsoleReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya-baca ke AWS WAF melalui. AWS Management Console Perhatikan bahwa kebijakan ini

juga memberikan izin untuk mencantumkan CloudFront distribusi Amazon, izin untuk melihat load balancer pada AWS Elastic Load Balancing, izin untuk melihat API dan tahapan REST Amazon API Gateway API, izin untuk mencantumkan dan melihat CloudWatch metrik Amazon, dan izin untuk melihat wilayah yang diaktifkan dalam akun.

Menggunakan kebijakan

Anda dapat melampirkan `AWSWAFConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 April 2020, 18:43 UTC
- Waktu yang telah diedit: 05 Juni 2023, 20.56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "apigateway:GET",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeRegions",
        "elasticloadbalancing:DescribeLoadBalancers",
```

```
        "appsync:ListGraphqlApis",
        "waf-regional:Get*",
        "waf-regional:List*",
        "waf:Get*",
        "waf:List*",
        "wafv2:Describe*",
        "wafv2:Get*",
        "wafv2:List*",
        "wafv2:CheckCapacity",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListResourcesForWebACL",
        "cognito-idp:GetWebACLForResource",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstances"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSWAFFullAccess

`AWSWAFFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke tindakan AWS WAF.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSWAFFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Oktober 2015, 20:44 UTC
- Waktu yang telah diedit: 05 Juni 2023, 20.55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFFullAccess`

Versi kebijakan

Versi kebijakan: v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "waf:*",
        "waf-regional:*",
        "wafv2:*",
        "elasticloadbalancing:SetWebACL",
        "apigateway:SetWebACL",
        "appsync:SetWebACL",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:ListResourcesForWebACL",
        "cognito-idp:GetWebACLForResource",
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListServices",
```

```
        "apprunner:ListAssociatedServicesForWebAcl",
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogDeliverySubscription",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSWAFReadOnlyAccess

`AWSWAFReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya baca ke tindakan AWS WAF.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSWAFReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Oktober 2015, 20:43 UTC
- Waktu yang telah diedit: 05 Juni 2023, 20.55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "wafv2:Get*",
        "wafv2:List*",
        "wafv2:Describe*",
        "wafv2:CheckCapacity",
        "cognito-idp:ListResourcesForWebACL",
        "cognito-idp:GetWebACLForResource",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSWellArchitectedDiscoveryServiceRolePolicy

`AWSWellArchitectedDiscoveryServiceRolePolicy`adalah kebijakanAWS terkelola yang: MemungkinkanWellArchitected untuk mengaksesAWS layanan dan sumber daya yang berhubungan denganWellArchitected sumber daya atas nama pelanggan.

Menggunakan kebijakan

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, grup, atau peran Anda.

Rincian

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 April 2023, 18:36 UTC
- Waktu yang telah diedit: 26 April 2023, 18.36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi standar adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeChecks",
        "trustedadvisor:DescribeCheckItems"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "resource-groups:ListGroupResources",
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:GetApplication",
        "servicecatalog:CreateAttributeGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup"
      ],
      "Resource" : [
        "arn:*:servicecatalog:*:*:/applications/*",
        "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:UpdateAttributeGroup",
        "servicecatalog:DeleteAttributeGroup"
      ],
      "Resource" : [
        "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSWellArchitectedOrganizationsServiceRolePolicy

`AWSWellArchitectedOrganizationsServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Well-Architected untuk mengakses Organizations atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 Juni 2022, 17:15 UTC
- Waktu yang telah diedit: 25 Juli 2022, 18.03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSWickrFullAccess

`AWSWickrFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin administratif penuh untuk layanan Wickr, termasuk fungsi administrasi Wickr di bawahAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSWickrFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 November 2022, 20:36 UTC
- Waktu yang telah diedit: 27 November 2022, 20.36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWickrFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wickr:*",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSXrayCrossAccountSharingConfiguration

`AWSXrayCrossAccountSharingConfiguration`adalah kebijakanAWS terkelola yang: Menyediakan kemampuan untuk mengelola tautan Observability Access Manager dan membangun berbagi jejak X-Ray

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSXrayCrossAccountSharingConfiguration` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 November 2022, 13:46 UTC
- Waktu yang telah diedit: 27 November 2022, 13.46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

AWSXRayDaemonWriteAccess

`AWSXRayDaemonWriteAccess`adalah kebijakan AWS terkelola yang: Izinkan Daemon AWS X-Ray menyampaikan data segmen jejak mentah ke API layanan dan mengambil data pengambilan sampel (aturan, target, dll.) untuk digunakan oleh X-Ray SDK.

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSXRayDaemonWriteAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 28 Agustus 2018, 23:00 UTC
- Waktu yang telah diedit: 13 Februari 2024, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSXrayFullAccess

`AWSXrayFullAccess`adalah kebijakan AWSterkelola yang: Kebijakan terkelola akses penuhAWS X-Ray

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSXrayFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Desember 2016, 18:30 UTC
- Waktu yang telah diedit: 01 Desember 2016 18.30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSXrayReadOnlyAccess

`AWSXrayReadOnlyAccess`adalah kebijakan AWS terkelola yang: AWS X-Ray hanya membaca kebijakan terkelola

Menggunakan kebijakan ini

Anda dapat melampirkan `AWSXrayReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Desember 2016, 18:27 UTC
- Waktu yang telah diedit: 14 Februari 2024, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXrayReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries",
        "xray:BatchGetTraces",
        "xray:BatchGetTraceSummaryById",
        "xray:GetDistinctTraceGraphs",
        "xray:GetServiceGraph",
        "xray:GetTraceGraph",
        "xray:GetTraceSummaries",
        "xray:GetGroups",
        "xray:GetGroup",
        "xray:ListTagsForResource",
        "xray:ListResourcePolicies",
        "xray:GetTimeSeriesServiceStatistics",
        "xray:GetInsightSummaries",
        "xray:GetInsight",
        "xray:GetInsightEvents",
        "xray:GetInsightImpactGraph"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

AWSXrayWriteOnlyAccess

`AWSXrayWriteOnlyAccess`adalah kebijakanAWS terkelola yang:AWS X-Ray menulis hanya kebijakan terkelola

Menggunakan kebijakan ini

Anda dapat melampirkan`AWSXrayWriteOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Desember 2016, 18:19 UTC
- Waktu yang telah diedit: 28 Agustus 2018 23.03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
```

```
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus menghapus penghapusan identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

AWSZonalAutoshiftPracticeRunSLRPolicy

`AWSZonalAutoshiftPracticeRunSLRPolicy`adalah kebijakan AWS terkelola yang: Menyediakan akses administratif untuk praktik pergeseran zona ARC, dan akses ke status CloudWatch alarm untuk memantau praktik berjalan.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 29 November 2023, 17:34 UTC
- Waktu telah diedit: 29 November 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MonitoringPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "health:DescribeEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ZonalShiftManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:CancelZonalShift",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:StartZonalShift",
        "arc-zonal-shift:UpdateZonalShift"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

BatchServiceRolePolicy

`BatchServiceRolePolicy`adalah kebijakan AWS terkelola yang: Menyediakan akses ke layanan AWS Batch untuk mengelola sumber daya yang diperlukan, termasuk sumber daya Amazon EC2 dan Amazon ECS.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Maret 2021, 06:55 UTC
- Waktu telah diedit: 05 Desember 2023, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBatchPolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
```

```
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:RequestSpotFleet",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "eks:DescribeCluster",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "ecs:DeregisterTaskDefinition",
        "ecs:TagResource",
        "ecs:ListAccountSettings",
        "logs:DescribeLogGroups",
        "iam:GetInstanceProfile",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement2",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
```

```
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/batch/job*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement3",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/batch/job*:log-stream:*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement4",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateOrUpdateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement5",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement6",
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "autoscaling.amazonaws.com",
            "ecs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CancelSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement9",
```

```
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteLaunchConfiguration"
      ],
      "Resource" :
 "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/AWSBatch*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement10",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:SuspendProcesses",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:TerminateInstanceInAutoScalingGroup"
      ],
      "Resource" : "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
AWSBatch*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement11",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteCluster",
        "ecs:DeregisterContainerInstance",
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/AWSBatch*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement12",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask"
      ],
      "Resource" : "arn:aws:ecs:*:*:task-definition/*"
```

```
    },
    {
      "Sid" : "AWSBatchPolicyStatement13",
      "Effect" : "Allow",
      "Action" : [
        "ecs:StopTask"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement14",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement15",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*:*:elastic-gpu/*",
        "arn:aws:elastic-inference:*:*:elastic-inference-accelerator/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
    },
    {
```

```
      "Sid" : "AWSBatchPolicyStatement16",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateLaunchTemplate",
            "RequestSpotFleet"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

Billing

`Billing`adalah kebijakan AWS terkelola yang: Memberikan izin untuk penagihan dan manajemen biaya. Ini termasuk melihat penggunaan akun dan melihat serta memodifikasi anggaran dan metode pembayaran.

Menggunakan kebijakan ini

Anda dapat melampirkan `Billing` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan fungsi Job
- Waktu pembuatan: 10 November 2016, 17:33 UTC
- Waktu telah diedit: 17 Januari 2024, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/Billing`

Versi kebijakan

Versi kebijakan: v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:*Billing",
        "aws-portal:*PaymentMethods",
        "aws-portal:*Usage",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
```

```
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billing:PutContractInformation",
        "billing:RedeemCredits",
        "billing:UpdateBillingPreferences",
        "billing:UpdateIAMAccessPreference",
        "budgets:CreateBudgetAction",
        "budgets:DeleteBudgetAction",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "budgets:ExecuteBudgetAction",
        "budgets:ModifyBudget",
        "budgets:UpdateBudgetAction",
        "budgets:ViewBudget",
        "ce:CreateCostCategoryDefinition",
        "ce:CreateNotificationSubscription",
        "ce:CreateReport",
        "ce:DeleteCostCategoryDefinition",
        "ce:DeleteNotificationSubscription",
        "ce:DeleteReport",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetCostAndUsage",
        "ce:ListCostAllocationTags",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "ce:TagResource",
        "ce:UpdateCostAllocationTagsStatus",
        "ce:UpdateNotificationSubscription",
        "ce:UpdatePreferences",
        "ce:UpdateReport",
        "ce:UpdateCostCategoryDefinition",
        "ce:UntagResource",
        "consolidatedbilling:GetAccountBillingRole",
        "consolidatedbilling:ListLinkedAccounts",
        "cur:DeleteReportDefinition",
        "cur:DescribeReportDefinitions",
        "cur:GetClassicReport",
```

```
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:ModifyReportDefinition",
        "cur:PutClassicReportPreferences",
        "cur:PutReportDefinition",
        "cur:ValidateReportDestination",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:PutFreeTierAlertPreference",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "invoicing:PutInvoiceEmailDeliveryPreferences",
        "payments:CreatePaymentInstrument",
        "payments:DeletePaymentInstrument",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentPreferences",
        "payments:MakePayment",
        "payments:UpdatePaymentPreferences",
        "pricing:DescribeServices",
        "purchase-orders:AddPurchaseOrder",
        "purchase-orders:DeletePurchaseOrder",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "purchase-orders:ModifyPurchaseOrders",
        "purchase-orders:TagResource",
        "purchase-orders:UntagResource",
        "purchase-orders:UpdatePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrderStatus",
        "purchase-orders:ViewPurchaseOrders",
        "support:CreateCase",
        "support:AddAttachmentsToSet",
        "sustainability:GetCarbonFootprintSummary",
        "tax:BatchPutTaxRegistration",
        "tax:DeleteTaxRegistration",
        "tax:GetExemptions",
        "tax:GetTaxInheritance",
        "tax:GetTaxInterview",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
```

```
        "tax:PutTaxInheritance",
        "tax:PutTaxInterview",
        "tax:PutTaxRegistration",
        "tax:UpdateExemptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CertificateManagerServiceRolePolicy

`CertificateManagerServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan Peran Layanan Certificate Manager Amazon

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

detail kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 25 Juni 2020
- Waktu yang telah diedit: 25 Juni 2020, 17.56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ClientVPNServiceConnectionsRolePolicy

`ClientVPNServiceConnectionsRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan untuk memungkinkanAWS Client VPN mengelola koneksi endpoint Client VPN Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Agustus 2020, 19:48 UTC
- Waktu yang telah diedit: 12 Agustus 2020 19.48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ClientVPNServiceRolePolicy

`ClientVPNServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan untuk memungkinkanAWS Client VPN mengelola endpoint Client VPN Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, grup, peran, peran, peran.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Desember 2018, 21:20 UTC
- Waktu yang telah diedit: 12 Agustus 2020 19.39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInternetGateways",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAccountAttributes",
        "ds:AuthorizeApplication",
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:UnauthorizeApplication",
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "acm:GetCertificate",
        "acm:DescribeCertificate",
        "iam:GetSAMLProvider",
        "lambda:GetFunctionConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

CloudFormationStackSetsOrgAdminServiceRolePolicy

`CloudFormationStackSetsOrgAdminServiceRolePolicy`adalah kebijakanAWS terkelola yang: Peran Layanan untuk CloudFormation StackSets (Akun Master Organisasi)

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Desember 2019, 00:20 UTC
- Waktu yang telah diedit: 10 Desember 2019, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsAWSOrganizationsReadAPIs",
      "Effect" : "Allow",
      "Action" : [
        "organizations:List*",
        "organizations:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeRoleInMemberAccounts",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/stacksets-exec-*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

CloudFormationStackSetsOrgMemberServiceRolePolicy

`CloudFormationStackSetsOrgMemberServiceRolePolicy`adalah kebijakanAWS terkelola yang: Peran Layanan untuk CloudFormation StackSets (Akun Anggota Organisasi)

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan pada pengguna, atau peran baru.

detail

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 09 Desember 2019, 23:52 UTC
- Waktu yang telah diedit: 09 Desember 2019 23.52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi atau atau atau atau atau atau atau atau atau Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
```

```
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/stacksets-exec-*"
      ]
    },
    {
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/stacksets-exec-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AdministratorAccess"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

CloudFrontFullAccess

`CloudFrontFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke CloudFront konsol ditambah kemampuan untuk membuat daftar bucket Amazon S3 melalui. AWS Management Console

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudFrontFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu telah diedit: 04 Januari 2024, 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfflistbuckets",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "cffullaccess",
      "Action" : [
        "acm:ListCertificates",
        "cloudfront:*",
        "cloudfront-keyvaluestore:*",
        "iam:ListServerCertificates",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
        "kinesis:ListStreams"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "cffdescribestream",
      "Action" : [
        "kinesis:DescribeStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:kinesis:*:*:*"
    },
    {
      "Sid" : "cfflistroles",
      "Action" : [
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudFrontReadOnlyAccess

`CloudFrontReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses ke informasi konfigurasi CloudFront distribusi dan daftar distribusi melalui. AWS Management Console

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudFrontReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu telah diedit: 04 Januari 2024, 16:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "iam:ListServerCertificates",
        "route53:List*",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudHSMServiceRolePolicy

`CloudHSMServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan akses keAWS sumber daya yang digunakan atau dikelola oleh CloudHSM

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran baru.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 06 November 2017, 19:12 UTC
- Waktu yang telah diedit: 06 November 2017 19.12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Kebijakan ini adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

CloudSearchFullAccess

`CloudSearchFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke layanan CloudSearch konfigurasi Amazon.

Menggunakan kebijakan ini

Anda dapat melampirkan`CloudSearchFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 18.39 UTC

- ARN: `arn:aws:iam::aws:policy/CloudSearchFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus izin identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

CloudSearchReadOnlyAccess

`CloudSearchReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke layanan CloudSearch konfigurasi Amazon.

Menggunakan kebijakan ini

Anda dapat melampirkan`CloudSearchReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 18.39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:Describe*",
        "cloudsearch:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

CloudTrailServiceRolePolicy

`CloudTrailServiceRolePolicy`adalah kebijakan AWS terkelola yang: Kebijakan izin untuk CloudTrail ServiceLinkedRole

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 Oktober 2018, 21:21 UTC
- Waktu telah diedit: November 27, 2023, 01:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailFullAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudtrail:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AwsOrgsDelegatedAdminAccess",
      "Effect" : "Allow",
      "Action" : "organizations:ListDelegatedAdministrators",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "cloudtrail.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteTableAccess",
      "Effect" : "Allow",
      "Action" : "glue:DeleteTable",
      "Resource" : [
        "arn:*:glue:*:*:catalog",
        "arn:*:glue:*:*:database/aws:cloudtrail",
        "arn:*:glue:*:*:table/aws:cloudtrail/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "DeregisterResourceAccess",
      "Effect" : "Allow",
      "Action" : "lakeformation:DeregisterResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatch-CrossAccountAccess

`CloudWatch-CrossAccountAccess`adalah kebijakanAWS terkelola yang: Memungkinkan CloudWatch untuk mengasumsikan CloudWatch -CrossAccountSharing peran dalam akun jarak jauh atas nama akun saat ini untuk menampilkan data lintas akun, lintas wilayah

Menggunakan kebijakan ini kebijakan kebijakan ini menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran tidak dapat dilampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

detail kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 Juli 2019, 09:59 UTC
- Waktu yang telah diedit: 23 Juli 2019 09.59 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan kebijakan kebijakan kebijakan kebijakan default kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan JSON JSON JSON JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

CloudWatchActionsEC2Access

`CloudWatchActionsEC2Access`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke CloudWatch alarm dan metrik serta metadata EC2. Menyediakan akses ke instans Stop, Terminate dan Reboot EC2.

Menggunakan kebijakan ini

Anda dapat melampirkan`CloudWatchActionsEC2Access` ke pengguna, grup, dan peran Anda.

detail kebijakan IAM

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 07 Juli 2015, 00:00 UTC
- Waktu yang telah diedit: 07 Juli 2015, 00.00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchActionsEC2Access`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

CloudWatchAgentAdminPolicy

`CloudWatchAgentAdminPolicy`adalah kebijakan AWS terkelola yang: Izin penuh diperlukan untuk digunakan AmazonCloudWatchAgent.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchAgentAdminPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Maret 2018, 00:52 UTC
- Waktu telah diedit: 05 Februari 2024, 20:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CWACloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:DescribeTags",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWASSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchAgentServerPolicy

`CloudWatchAgentServerPolicy`adalah kebijakan AWS terkelola yang: Izin yang diperlukan untuk digunakan AmazonCloudWatchAgent di server

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchAgentServerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 07 Maret 2018, 01:06 UTC
- Waktu telah diedit: 06 Februari 2024, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CWACloudWatchServerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:DescribeVolumes",
        "ec2:DescribeTags",
        "logs:PutLogEvents",
```

```
        "logs:PutRetentionPolicy",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWASSMServerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchApplicationInsightsFullAccess

`CloudWatchApplicationInsightsFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Wawasan CloudWatch Aplikasi dan dependensi yang diperlukan.

Menggunakan kebijakan ini

Anda dapat melampirkan`CloudWatchApplicationInsightsFullAccess` ke pengguna, grup, dan peran Anda.

detail

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 November 2020, 18:44 UTC
- Waktu yang telah diedit: 25 Januari 2022, 17.51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "sqs:ListQueues",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "autoscaling:DescribeAutoScalingGroups",
        "lambda:ListFunctions",
        "dynamodb:ListTables",
        "s3:ListAllMyBuckets",
```

```
        "sns:ListTopics",
        "states:ListStateMachines",
        "apigateway:GET",
        "ecs:ListClusters",
        "ecs:DescribeTaskDefinition",
        "ecs:ListServices",
        "ecs:ListTasks",
        "eks:ListClusters",
        "eks:ListNodegroups",
        "fsx:DescribeFileSystems",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

CloudWatchApplicationInsightsReadOnlyAccess

`CloudWatchApplicationInsightsReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke CloudWatch Application Insights.

Menggunakan kebijakan ini

Anda dapat melampirkan`CloudWatchApplicationInsightsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 November 2020, 18:48 UTC
- Waktu yang telah diedit: 24 November 2020 18.48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

CloudwatchApplicationInsightsServiceLinkedRolePolicy

`CloudwatchApplicationInsightsServiceLinkedRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan Peran Tertaut Layanan Wawasan Aplikasi Cloudwatch

Menggunakan kebijakan ini menggunakan kebijakan ini menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini tidak dapat melampirkan kebijakan ini tidak dapat melampirkan kebijakan ini tidak dapat melampirkan kebijakan ini tidak dapat melampirkan kebijakan ini tidak dapat melampirkan kebijakan ini

Kebijakan tidak dapat dilampirkan rincian

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 01 Desember 2018, 16:22 UTC
- Waktu yang telah diedit: 11 Mei 2023, 16.34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan:v24 (default)

Kebijakan tidak dapat dilampirkan versi yang menentukan izin untuk kebijakan tidak dapat dilampirkan pada versi yang mengizinkan kebijakan tidak dapat dilampirkan pada versi yang

menentukan izin kebijakan tidak dapat dilampirkan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan SON SON SON SON SON SON SON SON SON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:PutAnomalyDetector",
        "cloudwatch:DeleteAnomalyDetector",
        "cloudwatch:DescribeAnomalyDetectors"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudFormation:CreateStack",
        "cloudFormation:UpdateStack",
        "cloudFormation:DeleteStack",
        "cloudFormation:DescribeStackResources"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudFormation:DescribeStacks",
        "cloudFormation:ListStackResources",
        "cloudFormation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetGroup"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/ApplicationInsights-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-ApplicationInsights-*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AmazonCloudWatch-ManageAgent"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:CreateOpsItem",
        "ssm:DescribeOpsItems",
        "ssm:UpdateOpsItem",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommandInvocations",
        "ssm:GetCommandInvocation"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AWSEC2-CheckPerformanceCounterSets",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AWSEC2-DetectWorkload",
        "arn:aws:ssm:*:*:document/AmazonCloudWatch-ManageAgent"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeNatGateways"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions",
        "lambda:GetFunctionConfiguration",
```

```
        "lambda:ListEventSourceMappings"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AmazonCloudWatch-ApplicationInsights-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph",
        "xray:GetTraceSummaries",
        "xray:GetTimeSeriesServiceStatistics",
        "xray:GetTraceGraph"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeTimeToLive"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "application-autoscaling:DescribeScalableTargets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetMetricsConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:DescribeExecution",
        "states:DescribeStateMachine",
        "states:GetExecutionHistory"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
```

```
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "ecs:ListTasks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateClusterSettings"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:GetSMSAttributes",
```

```
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteSubscriptionFilter"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutSubscriptionFilter"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*",
        "arn:aws:logs:*:*:destination:AmazonCloudWatch-ApplicationInsights-
LogIngestionDestination*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFileSystems"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHealthCheck",
        "route53:ListHostedZones",
        "route53:ListHealthChecks",
        "route53:ListQueryLoggingConfigs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetFirewallRuleGroupAssociation"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

CloudWatchApplicationSignalsServiceRolePolicy

`CloudWatchApplicationSignalsServiceRolePolicy`adalah kebijakan AWS terkelola yang: Kebijakan memberikan izin kepada Sinyal CloudWatch Aplikasi untuk mengumpulkan data pemantauan dan penandaan dari layanan terkait AWS lainnya.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 09 November 2023, 18:09 UTC
- Waktu telah diedit: 07 Maret 2024, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "XRayPermission",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph"
      ],
```

```
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWLogsPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/appsignals/*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWMetricsPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagsPermission",
      "Effect" : "Allow",
```

```
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchAutomaticDashboardsAccess

`CloudWatchAutomaticDashboardsAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses keCloudWatch non-API yang digunakan untuk menampilkan Dasbor CloudWatch Otomatis, termasuk isi objek seperti fungsi Lambda

Menggunakan kebijakan ini

Anda dapat melampirkan`CloudWatchAutomaticDashboardsAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 23 Juli 2019, 10:01 UTC
- Waktu yang telah diedit: 20 April 2021 13.05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudfront:GetDistribution",
        "cloudfront:ListDistributions",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "elasticache:DescribeCacheClusters",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "lambda:GetFunction",
        "lambda:ListFunctions",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
```

```
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListQueues",
        "synthetics:DescribeCanariesLastRun",
        "tag:GetResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "apigateway:GET"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:apigateway:*::/restapis*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

CloudWatchCrossAccountSharingConfiguration

`CloudWatchCrossAccountSharingConfiguration`adalah kebijakanAWS terkelola yang: Menyediakan kemampuan untuk mengelola tautan Pengamatan Access Manager dan membangun berbagi CloudWatch sumber daya

Menggunakan kebijakan ini

Anda dapat melampirkan`CloudWatchCrossAccountSharingConfiguration` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 November 2022, 14:01 UTC
- Waktu yang telah diedit: 27 November 2022, 14.01 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

CloudWatchEventsBuiltInTargetExecutionAccess

`CloudWatchEventsBuiltInTargetExecutionAccess`kebijakanAWS terkelola yang memungkinkan built-in target di Amazon CloudWatch Events untuk melakukan tindakan EC2 atas nama Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`CloudWatchEventsBuiltInTargetExecutionAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 14 Januari 2016, 18:35 UTC
- Waktu yang telah diedit: 14 Januari 2016 18.35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

CloudWatchEventsFullAccess

`CloudWatchEventsFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon CloudWatch Events.

Menggunakan kebijakan ini

Anda dapat melampirkan`CloudWatchEventsFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 14 Januari 2016, 18:37 UTC
- Waktu yang telah diedit: 01 Desember 2022, 17.05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
AmazonEventBridgeApiDestinationsServiceRolePolicy",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "apidestinations.events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "schemas.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccessForApiDestinations",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!*"
    },
    {
      "Sid" : "IAMPassRoleForCloudWatchEvents",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS_Events_Invoke_Targets"
    },
    {
      "Sid" : "IAMPassRoleAccessForScheduler",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

CloudWatchEventsInvocationAccess

`CloudWatchEventsInvocationAccess`adalah kebijakanAWS terkelola yang: Memungkinkan Amazon CloudWatch Events menyampaikan peristiwa ke aliran diAWS Kinesis Streams di akun Anda.

Menggunakan kebijakan ini

Anda dapat melampirkan`CloudWatchEventsInvocationAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan

- Waktu pembuatan: 14 Januari 2016, 18:36 UTC
- Waktu yang telah diedit: 14 Januari 2016 18.36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsInvocationAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

CloudWatchEventsReadOnlyAccess

`CloudWatchEventsReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya baca ke Amazon CloudWatch Events.

Menggunakan kebijakan

Anda dapat melampirkan`CloudWatchEventsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Detail

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 14 Januari 2016, 18:27 UTC
- Waktu yang diedit: 01 Desember 2022, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DescribeEventBus",
        "events:DescribeEventSource",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
```

```
        "events:ListTargetsByRule",
        "events:TestEventPattern",
        "events:DescribeArchive",
        "events:ListArchives",
        "events:DescribeReplay",
        "events:ListReplays",
        "events:DescribeConnection",
        "events:ListConnections",
        "events:DescribeApiDestination",
        "events:ListApiDestinations",
        "events:DescribeEndpoint",
        "events:ListEndpoints",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:ExportSchema",
        "schemas:GetCodeBindingSource",
        "schemas:GetDiscoveredSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "schemas:SearchSchemas",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

CloudWatchEventsServiceRolePolicy

`CloudWatchEventsServiceRolePolicy`adalah kebijakanAWS terkelola yang: IzinkanAWS CloudWatch untuk mengeksekusi tindakan atas nama Anda yang dikonfigurasi melalui alarm dan peristiwa.

Menggunakan kebijakan ini kebijakan ini kebijakan ini kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan yang mengizinkan layanan yang mengizinkan layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, grup, grup, grup, grup, grup, grup, grup, grup, grup, atau peran Anda

Rincian kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 November 2017, 00:42 UTC
- Waktu yang telah diedit: 17 November 2017, 00.42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan ini versi yang menentukan izin untuk kebijakan kebijakan kebijakan kebijakan ini. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

CloudWatchFullAccess

`CloudWatchFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke CloudWatch.

Menggunakan kebijakan ini

Anda dapat melampirkan`CloudWatchFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC

- Waktu penyuntingan: 27 November 2022, 13:23 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudwatch:*",
        "logs:*",
        "sns:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "oam:ListSinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "events.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan menghapus dan
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

CloudWatchFullAccessV2

`CloudWatchFullAccessV2`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke CloudWatch.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchFullAccessV2` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 01 Agustus 2023, 11:32 UTC
- Waktu telah diedit: 05 Desember 2023, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccessV2`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "cloudwatch:*",
        "logs:*",
        "sns:CreateTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "oam:ListSinks",
        "rum:*",
        "synthetics:*",
        "xray:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "EventsServicePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchInternetMonitorServiceRolePolicy

`CloudWatchInternetMonitorServiceRolePolicy`adalahAWSkebijakan terkelolabahwa: Memungkinkan Internet Monitor untuk mengakses EC2, Workspace, danCloudFrontsumber daya, dan layanan lain yang diperlukan atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 27 November 2022, 17:46 UTC
- Waktu yang diedit:20 Juli 2023, 04:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/internet-monitor/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/internet-monitor/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/InternetMonitor"
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai denganAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

CloudWatchLambdaInsightsExecutionRolePolicy

`CloudWatchLambdaInsightsExecutionRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan yang diperlukan untuk Ekstensi Lambda Insights

Menggunakan kebijakan ini

Anda dapat melampirkan`CloudWatchLambdaInsightsExecutionRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 07 Oktober 2020, 19:27 UTC
- Waktu yang telah diedit: 07 Oktober 2020 19.27 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda-insights:*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

CloudWatchLogsCrossAccountSharingConfiguration

`CloudWatchLogsCrossAccountSharingConfiguration`adalah kebijakanAWS terkelola yang: Menyediakan kemampuan untuk mengelola tautan Pengamatan Access Manager dan membangun berbagi sumber daya CloudWatch Log

Menggunakan kebijakan ini

Anda dapat melampirkan`CloudWatchLogsCrossAccountSharingConfiguration` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 November 2022, 13:55 UTC
- Waktu yang telah diedit: 27 November 2022, 13.55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

CloudWatchLogsFullAccess

`CloudWatchLogsFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke CloudWatch Log

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchLogsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 26 November 2023, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchLogsReadOnlyAccess

`CloudWatchLogsReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya baca ke CloudWatch Log

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchLogsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 26 November 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchNetworkMonitorServiceRolePolicy

`CloudWatchNetworkMonitorServiceRolePolicy`adalah kebijakan AWS terkelola yang: Memungkinkan Monitor CloudWatch Jaringan untuk mengakses dan mengelola sumber daya EC2 dan VPC, mempublikasikan data CloudWatch ke dan mengakses layanan lain yang diperlukan atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 21 Desember 2023, 18:53 UTC
- Waktu yang telah diedit: 21 Desember 2023, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PublishCw",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NetworkMonitor"
        }
      }
    },
```

```
    {
      "Sid" : "DescribeAny",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteModifyEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedByCloudWatchNetworkMonitor" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchReadOnlyAccess

`CloudWatchReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya baca CloudWatch.

Menggunakan kebijakan ini

Anda dapat melampirkan `CloudWatchReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu telah diedit: 05 Desember 2023, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "autoscaling:Describe*",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
```

```
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "oam:ListSinks",
        "sns:Get*",
        "sns:List*",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "xray:BatchGet*",
        "xray:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CloudWatchSyntheticsFullAccess

`CloudWatchSyntheticsFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke CloudWatch Synthetics.

Menggunakan kebijakan ini

Anda dapat melampirkan`CloudWatchSyntheticsFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 25 November 2019, 17:39 UTC
- Waktu yang telah diedit: 06 Mei 2022, 18.14 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess`

Versi kebijakan

Versi kebijakan:v9 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::cw-syn-results-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces",
        "apigateway:GET"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::cw-syn-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::aws-synthetics-library-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "synthetics.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:Synthetics-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:GetFunctionConfiguration",
        "lambda:DeleteFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:cwsyn-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetLayerVersion",
        "lambda:PublishLayerVersion",
        "lambda:DeleteLayerVersion"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:layer:cwsyn-*",
        "arn:aws:lambda:*:*:layer:Synthetics:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "arn:*:sns:*:*:Synthetics-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com"
```

```
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

CloudWatchSyntheticsReadOnlyAccess

`CloudWatchSyntheticsReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke CloudWatch Synthetics.

Menggunakan kebijakan ini

Anda dapat melampirkan`CloudWatchSyntheticsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 25 November 2019, 17:45 UTC
- Waktu yang telah diedit: 06 Maret 2020, 19.26 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

ComprehendDataAccessRolePolicy

`ComprehendDataAccessRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan untukAWS Comprehend peran layanan yang memungkinkan akses ke sumber daya S3 untuk akses data

Menggunakan kebijakan ini

Anda dapat melampirkan`ComprehendDataAccessRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Maret 2019, 22:28 UTC
- Waktu yang telah diedit: 06 Maret 2019, 22.28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*Comprehend*",
      "arn:aws:s3:::*comprehend*"
    ]
  }
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ComprehendFullAccess

`ComprehendFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Comprehend.

Menggunakan kebijakan ini

Anda dapat melampirkan`ComprehendFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 November 2017, 18:08 UTC
- Waktu yang telah diedit: 05 Desember 2017 01.36 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ComprehendMedicalFullAccess

`ComprehendMedicalFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Comprehend Medical

Menggunakan kebijakan ini

Anda dapat melampirkan`ComprehendMedicalFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 November 2018, 17:55 UTC
- Waktu yang telah diedit: 27 November 2018 07.55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehendmedical:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ComprehendReadOnly

`ComprehendReadOnly`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke Amazon Comprehend.

Menggunakan kebijakan ini

Anda dapat melampirkan`ComprehendReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 November 2017, 18:10 UTC
- Waktu yang telah diedit: 26 April 2022, 21.32 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendReadOnly`

Versi kebijakan

Versi kebijakan:v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectDominantLanguage",
        "comprehend:BatchDetectDominantLanguage",
        "comprehend:DetectEntities",
        "comprehend:BatchDetectEntities",
        "comprehend:DetectKeyPhrases",
        "comprehend:BatchDetectKeyPhrases",
        "comprehend:DetectPiiEntities",
        "comprehend:ContainsPiiEntities",
        "comprehend:DetectSentiment",
        "comprehend:BatchDetectSentiment",
        "comprehend:DetectSyntax",
        "comprehend:BatchDetectSyntax",
        "comprehend:ClassifyDocument",
        "comprehend:DescribeTopicsDetectionJob",
        "comprehend:ListTopicsDetectionJobs",
        "comprehend:DescribeDominantLanguageDetectionJob",
        "comprehend:ListDominantLanguageDetectionJobs",
        "comprehend:DescribeEntitiesDetectionJob",
        "comprehend:ListEntitiesDetectionJobs",
        "comprehend:DescribeKeyPhrasesDetectionJob",
        "comprehend:ListKeyPhrasesDetectionJobs",
        "comprehend:DescribePiiEntitiesDetectionJob",
        "comprehend:ListPiiEntitiesDetectionJobs",
        "comprehend:DescribeSentimentDetectionJob",
        "comprehend:DescribeTargetedSentimentDetectionJob",
        "comprehend:ListSentimentDetectionJobs",
        "comprehend:ListTargetedSentimentDetectionJobs",
```

```
        "comprehend:DescribeDocumentClassifier",
        "comprehend:ListDocumentClassifiers",
        "comprehend:DescribeDocumentClassificationJob",
        "comprehend:ListDocumentClassificationJobs",
        "comprehend:DescribeEntityRecognizer",
        "comprehend:ListEntityRecognizers",
        "comprehend:ListTagsForResource",
        "comprehend:DescribeEndpoint",
        "comprehend:ListEndpoints",
        "comprehend:ListDocumentClassifierSummaries",
        "comprehend:ListEntityRecognizerSummaries",
        "comprehend:DescribeResourcePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

ComputeOptimizerReadOnlyAccess

`ComputeOptimizerReadOnlyAccess`adalah sebuahAWSkebijakan terkelolaitu: Menyediakan akses baca saja ke ComputeOptimizer.

Menggunakan kebijakan ini

Anda dapat melampirkan`ComputeOptimizerReadOnlyAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 07 Maret 2020, 00:11 UTC

- Waktu yang diedit:28 Agustus 2023, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v7(default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetRecommendationSummaries",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetLicenseRecommendations",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:ListServices",
        "ecs:ListClusters",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "lambda:ListFunctions",
```

```
        "lambda:ListProvisionedConcurrencyConfigs",
        "cloudwatch:GetMetricData",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai denganAWSkebijakan terkelola dan beralih ke izin hak istimewa paling sedikit

ComputeOptimizerServiceRolePolicy

`ComputeOptimizerServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan ComputeOptimizer untuk memanggilAWS layanan dan mengumpulkan rincian beban kerja atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 03 Desember 2019, 08:45 UTC
- Waktu yang telah diedit: 13 Juni 2022, 19.05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ComputeOptimizerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AutoScalingAccess",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2Access",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

ConfigConformsServiceRolePolicy

`ConfigConformsServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan yang diperlukan AWSConfig untuk membuat paket kesesuaian

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 25 Juli 2019, 21:38 UTC

- Waktu yang telah diedit: 12 Januari 2023, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/config-
conforms.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeRemediationConfigurations",
        "config:DeleteRemediationConfiguration",
        "config:PutRemediationConfigurations"
      ],
```

```
      "Resource" : "arn:aws:config:*:*:remediation-configuration/aws-service-
remediation-configuration/config-conforms.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "remediation.config.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
```

```
        "ssm:GetDocument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:GetObject",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::awsconfigconforms*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetStackPolicy",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:ValidateTemplate",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/awsconfigconforms-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Config"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

CostOptimizationHubAdminAccess

`CostOptimizationHubAdminAccess`adalah kebijakan AWS terkelola yang: Kebijakan terkelola ini menyediakan akses admin ke Hub Pengoptimalan Biaya.

Menggunakan kebijakan ini

Anda dapat melampirkan `CostOptimizationHubAdminAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Desember 2023, 00:03 UTC
- Waktu yang telah diedit: 19 Desember 2023, 00:03 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "CostOptimizationHubAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:UpdateEnrollmentStatus",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:UpdatePreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/cost-optimization-hub.bcm.amazonaws.com/
AWSServiceRoleForCostOptimizationHub"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cost-optimization-hub.bcm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceAccessForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "cost-optimization-hub.bcm.amazonaws.com"
          ]
        }
      }
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CostOptimizationHubReadOnlyAccess

`CostOptimizationHubReadOnlyAccess`adalah kebijakan AWS terkelola yang: Kebijakan terkelola ini menyediakan akses hanya-baca ke Hub Pengoptimalan Biaya.

Menggunakan kebijakan ini

Anda dapat melampirkan `CostOptimizationHubReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 Desember 2023, 18:04 UTC
- Waktu yang telah diedit: 13 Desember 2023, 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CostOptimizationHubServiceRolePolicy

`CostOptimizationHubServiceRolePolicy`adalah kebijakan AWS terkelola yang: Memungkinkan Hub Pengoptimalan Biaya untuk mengambil informasi organisasi dan mengumpulkan data dan metadata terkait pengoptimalan.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 26 November 2023, 08:03 UTC
- Waktu telah diedit: 26 November 2023, 08:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CostExplorerAccess",
      "Effect" : "Allow",
      "Action" : [
        "ce:ListCostAllocationTags"
```

```
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

CustomerProfilesServiceLinkedRolePolicy

`CustomerProfilesServiceLinkedRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Profil Pelanggan Amazon Connect mengaksesAWS layanan dan sumber daya atas nama Anda.

Menggunakan menggunakan menggunakan menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna,,,,,,,,,,,,,,,,,,,,,

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 Maret 2023, 22:56 UTC
- Waktu yang telah diedit: 07 Maret 2023, 22.56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/CustomerProfiles"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/profile.amazonaws.com/
AWSServiceRoleForProfile_*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

DatabaseAdministrator

`DatabaseAdministrator`adalah kebijakanAWS terkelola yang: Memberikan izin akses penuh keAWS layanan dan tindakan yang diperlukan untuk menyiapkan dan mengonfigurasi layananAWS database.

Menggunakan kebijakan ini

Anda dapat melampirkan`DatabaseAdministrator` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan fungsi Job
- Waktu pembuatan: 10 November 2016, 17:25 UTC
- Waktu yang telah diedit: 08 Januari 2019 08.48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DatabaseAdministrator`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:Describe*",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:PutMetricAlarm",
```

```
        "datapipeline:ActivatePipeline",
        "datapipeline:CreatePipeline",
        "datapipeline:DeletePipeline",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:PutPipelineDefinition",
        "datapipeline:QueryObjects",
        "dynamodb:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticache:*",
        "iam:ListRoles",
        "iam:GetRole",
        "kms:ListKeys",
        "lambda:CreateEventSourceMapping",
        "lambda:CreateFunction",
        "lambda:DeleteEventSourceMapping",
        "lambda:DeleteFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:Create*",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "rds:*",
        "redshift:*",
        "s3:CreateBucket",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Get*",
        "sns:List*",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
```

```
        "sns:Unsubscribe"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject*",
        "s3:Get*",
        "s3:List*",
        "s3:PutAccelerateConfiguration",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutBucketWebsite",
        "s3:PutLifecycleConfiguration",
        "s3:PutReplicationConfiguration",
        "s3:PutObject*",
        "s3:Replicate*",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/rds-monitoring-role",
        "arn:aws:iam::*:role/rdbms-lambda-access",
        "arn:aws:iam::*:role/lambda_exec_role",
        "arn:aws:iam::*:role/lambda-dynamodb-*",
        "arn:aws:iam::*:role/lambda-vpc-execution-role",
        "arn:aws:iam::*:role/DataPipelineDefaultRole",
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

DataScientist

`DataScientist`adalah kebijakanAWS terkelola yang: Memberikan izin ke layanan analisisAWS data.

Menggunakan kebijakan ini

Anda dapat melampirkan`DataScientist` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan fungsi Job
- Waktu pembuatan: 10 November 2016, 17:28 UTC
- Waktu yang telah diedit: 03 Desember 2019 16.48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DataScientist`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Action" : [
        "autoscaling:*",
        "cloudwatch:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "datapipeline:Describe*",
        "datapipeline:ListPipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:QueryObjects",
        "dynamodb:*",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CancelSpotFleetRequests",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySpotFleetRequest",
        "ec2:RequestSpotInstances",
        "ec2:RequestSpotFleet",
        "elasticfilesystem:*",
        "elasticmapreduce:*",
        "es:*",
        "firehose:*",
        "fsx:DescribeFileSystems",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListRoles",
        "kinesis:*",
        "kms:List*",
        "lambda:Create*",
        "lambda:Delete*",
        "lambda:Get*",
        "lambda:InvokeFunction",
        "lambda:PublishVersion",
        "lambda:Update*",
        "lambda:List*",
        "machinelearning:*",
        "sdb:*",
        "rds:*",
        "sns:ListSubscriptions",
        "sns:ListTopics",
```

```
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "redshift:*",
        "s3:CreateBucket",
        "sns:CreateTopic",
        "sns:Get*",
        "sns:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Abort*",
        "s3:DeleteObject",
        "s3:Get*",
        "s3:List*",
        "s3:PutAccelerateConfiguration",
        "s3:PutBucketCors",
        "s3:PutBucketLogging",
        "s3:PutBucketNotification",
        "s3:PutBucketTagging",
        "s3:PutObject",
        "s3:Replicate*",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultRole",
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
        "arn:aws:iam::*:role/EMR_DefaultRole",
        "arn:aws:iam::*:role/kinesis-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListUserProfiles",
        "sagemaker:*App",
        "sagemaker:ListApps"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

DAXServiceRolePolicy

`DAXServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memungkinkan DAX untuk membuat dan mengelola antarmuka Jaringan, Grup keamanan, Subnet dan Vpc atas nama pelanggan

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, atau peran baru.

detail kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 Maret 2018, 17:51 UTC
- Waktu yang telah diedit: 05 Maret 2018 07.51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan default adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan kebijakan kebijakan kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

`DynamoDBCloudWatchContributorInsightsServiceRolePolicy`adalah kebijakanAWS terkelola yang: Izin yang diperlukan untuk mendukung Amazon CloudWatch Contributor Insights for Amazon DynamoDB.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 15 November 2019, 21:13 UTC
- Waktu yang telah diedit: 15 November 2019, 21.13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DeleteInsightRules",
        "cloudwatch:PutInsightRule"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Action" : [
        "cloudwatch:DescribeInsightRules"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

DynamoDBKinesisReplicationServiceRolePolicy

`DynamoDBKinesisReplicationServiceRolePolicy`adalah kebijakanAWS terkelola yang: Menyediakan aksesAWS DynamoDB KinesisDataStreams

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 November 2020, 00:43 UTC
- Waktu yang telah diedit: 12 November 2020, 00:43 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "kinesis.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

DynamoDBReplicationServiceRolePolicy

`DynamoDBReplicationServiceRolePolicy`adalah kebijakan AWS terkelola yang: Izin yang diperlukan oleh DynamoDB untuk replikasi data lintas wilayah

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 09 November 2017, 23:55 UTC
- Waktu telah diedit: 08 Januari 2024, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v8 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBActionsNeededForSteadyStateReplication",
      "Effect" : "Allow",
      "Action" : [
```

```
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteItem",
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "dynamodb:Scan",
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:UpdateTimeToLive",
        "dynamodb:DescribeLimits",
        "dynamodb:GetResourcePolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DescribeScalingPolicies",
        "account:ListRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBReplicationServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

EC2FastLaunchServiceRolePolicy

`EC2FastLaunchServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan memberikan ec2fastlaunch untuk mempersiapkan dan mengelola snapshot preprovisioned di akun pelanggan & mempublikasikan metrik terkait.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, atau peran.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 10 Januari 2022, 13:08 UTC
- Waktu yang telah diedit: 10 Januari 2022, 13.08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateTaggedSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "StringLike" : {
          "aws:RequestTag/CreatedByLaunchTemplateVersion" : "*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "CreatedByLaunchTemplateName",
            "CreatedByLaunchTemplateId"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSnapshot",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/EC2"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

EC2FleetTimeShiftableServiceRolePolicy

`EC2FleetTimeShiftableServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan memberikan izin kepada Armada EC2 untuk meluncurkan instans di future.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini.

detail

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 23 Desember 2019, 19:47 UTC
- Waktu yang telah diedit: 23 Desember 2019 19.47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi kebijakan terterterterterterterterterterterterterterterterterterterterterterterterterterterterterterterterterterterterterter. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstances",
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2:fleet-id" : "*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

Ec2ImageBuilderCrossAccountDistributionAccess

`Ec2ImageBuilderCrossAccountDistributionAccess`adalah kebijakanAWS terkelola yang: Izin yang dibutuhkan oleh EC2 Image Builder untuk melakukan distribusi lintas akun.

Menggunakan kebijakan ini

Anda dapat melampirkan`Ec2ImageBuilderCrossAccountDistributionAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 September 2020, 19:22 UTC
- Waktu yang telah diedit: 30 September 2020 19.22 UTC
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*::image/*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeImages",
        "ec2:CopyImage",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

EC2ImageBuilderLifecycleExecutionPolicy

`EC2ImageBuilderLifecycleExecutionPolicy`adalah kebijakan AWS terkelola yang: Kebijakan EC2 ImageBuilderLifecycleExecutionPolicy memberikan izin kepada Image Builder untuk melakukan tindakan seperti menghentikan atau menghapus sumber daya gambar Image Builder dan sumber daya dasarnya (AMI, snapshot) untuk mendukung aturan otomatis untuk tugas manajemen siklus hidup gambar.

Menggunakan kebijakan ini

Anda dapat melampirkan `EC2ImageBuilderLifecycleExecutionPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 16 November 2023, 23:23 UTC
- Waktu telah diedit: 16 November 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImage",
        "ec2:DeregisterImage",
        "ec2:EnableImageDeprecation",
        "ec2:DescribeImageAttribute",
        "ec2:DisableImage",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
```

```
      "Sid" : "EC2TagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeprecatedBy" : "EC2 Image Builder",
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "DeprecatedBy"
        }
      }
    },
    {
      "Sid" : "ECRImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:BatchDeleteImage"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "StringEquals" : {
          "ecr:ResourceTag/LifecycleExecutionAccess" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "ImageBuilderEC2TagServicePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "tag:GetResources",
        "imagebuilder:DeleteImage"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

EC2InstanceConnect

`EC2InstanceConnect`adalah kebijakanAWS terkelola yang: Memungkinkan pelanggan untuk memanggil EC2 Instance Connect untuk mempublikasikan kunci sementara ke instans EC2 mereka dan terhubung melalui ssh atau EC2 Instance Connect CLI.

Menggunakan kebijakan ini

Anda dapat melampirkan`EC2InstanceConnect` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 Juni 2019, 18:53 UTC
- Waktu yang telah diedit: 27 Juni 2019 18.53 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

Ec2InstanceConnectEndpoint

`Ec2InstanceConnectEndpoint`adalah kebijakanAWS terkelola yang: EC2 Instance Connect kebijakan endpoint untuk mengelola EC2 Instans Connect endpoint yang dibuat oleh pelanggan

Menggunakan kebijakan ini terkait kebijakan ini terkait kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, peran, atau peran Anda.

detail detail kebijakan kebijakan kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan

- Waktu pembuatan: 24 Januari 2023, 20:19 UTC
- Waktu yang telah diedit: 24 Januari 2023, 20.19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan ini adalah versi yang menentukan izin untuk kebijakan default. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON SON SON SON SON SON SON SON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "InstanceConnectEndpointId"
          ]
        },
        "Null" : {
          "aws:RequestTag/InstanceConnectEndpointId" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "InstanceConnectEndpointId"
          ]
        },
        "Null" : {
          "aws:RequestTag/InstanceConnectEndpointId" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

EC2InstanceProfileForImageBuilder

`EC2InstanceProfileForImageBuilder`adalah kebijakanAWS terkelola yang: Profil Instans EC2 untuk layanan Image Builder.

Menggunakan kebijakan ini

Anda dapat melampirkan`EC2InstanceProfileForImageBuilder` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 Desember 2019, 19:08 UTC
- Waktu yang telah diedit: 27 Agustus 2020, 16.40 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:imagebuilder:arn",
          "aws:CalledVia" : [
            "imagebuilder.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::ec2imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
```

```
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

EC2InstanceProfileForImageBuilderECRContainerBuilds

`EC2InstanceProfileForImageBuilderECRContainerBuilds`adalah kebijakanAWS terkelola yang: Profil Instans EC2 untuk membangun gambar kontainer dengan EC2 Image Builder. Kebijakan ini memberikan izin luas kepada pengguna untuk mengunggah gambar ECR.

Menggunakan kebijakan ini

Anda dapat melampirkan`EC2InstanceProfileForImageBuilderECRContainerBuilds` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 11 Desember 2020, 19.48 UTC
- Waktu yang telah diedit: 11 Desember 2020 19.48 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:PutImage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:imagebuilder:arn",
          "aws:CalledVia" : [
            "imagebuilder.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::ec2imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

ECRReplicationServiceRolePolicy

`ECRReplicationServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan akses keLayanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Replikasi ECR

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 04 Desember 2020, 22:11 UTC

- Waktu yang telah diedit: 04 Desember 2020, 22.11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

ElastiCacheServiceRolePolicy

`ElastiCacheServiceRolePolicy`adalah kebijakan AWS terkelola yang: Kebijakan ini memungkinkan ElastiCache untuk mengelola AWS sumber daya atas nama Anda sebagaimana diperlukan untuk mengelola cache Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 Desember 2017, 17:50 UTC
- Waktu telah diedit: 28 November 2023, 03:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "cloudwatch:PutMetricData",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDeleteVPCEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
        }
      }
    },
    {
      "Sid" : "TagVPCEndpointsOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAccessToElastiCacheTaggedVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ElasticLoadBalancingFullAccess

`ElasticLoadBalancingFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon ElasticLoadBalancing, dan akses terbatas ke layanan lain yang diperlukan untuk menyediakan ElasticLoadBalancing fitur.

Menggunakan kebijakan ini

Anda dapat melampirkan`ElasticLoadBalancingFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 20 September 2018, 20:42 UTC
- Waktu yang telah diedit: 29 November 2022, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

Versi kebijakan

Versi kebijakan:v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:DescribeVpcPeeringConnections",
        "cognito-idp:DescribeUserPoolClient"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "arc-zonal-shift:*",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

ElasticLoadBalancingReadOnly

`ElasticLoadBalancingReadOnly`adalah kebijakan AWS terkelola yang: Menyediakan akses baca saja ke Amazon ElasticLoadBalancing dan layanan dependen

Menggunakan kebijakan ini

Anda dapat melampirkan `ElasticLoadBalancingReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 20 September 2018, 20:17 UTC
- Waktu telah diedit: 26 November 2023, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Statement2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeClassicLinkInstances",
```

```
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Statement3",
      "Effect" : "Allow",
      "Action" : "arc-zonal-shift:GetManagedResource",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    },
    {
      "Sid" : "Statement4",
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ElementalActivationsDownloadSoftwareAccess

`ElementalActivationsDownloadSoftwareAccess`adalah kebijakanAWS terkelola yang: Akses untuk melihat aset yang dibeli dan mengunduh perangkat lunak terkait dan file kickstart

Menggunakan kebijakan ini

Anda dapat melampirkan`ElementalActivationsDownloadSoftwareAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 08 September 2020, 17:26 UTC
- Waktu yang telah diedit: 08 September 2020, 17.26 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:Download*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

ElementalActivationsFullAccess

`ElementalActivationsFullAccess`adalah kebijakanAWS terkelola yang: Akses penuh untuk melihat dan mengambil tindakan pada aset yang dibeli Peralatan dan Perangkat Lunak Elemental

Menggunakan kebijakan ini

Anda dapat melampirkan`ElementalActivationsFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 04 Juni 2020, 21:00 UTC
- Waktu yang telah diedit: 04 Juni 2020, 21.00 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ElementalActivationsGenerateLicenses

`ElementalActivationsGenerateLicenses`adalah kebijakanAWS terkelola yang: Akses untuk melihat aset yang dibeli dan menghasilkan lisensi perangkat lunak untuk aktivasi yang tertunda

Menggunakan kebijakan

Anda dapat melampirkan`ElementalActivationsGenerateLicenses` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 28 Agustus 2020, 18:28 UTC
- Waktu yang telah diedit: 28 Agustus 2020 08.28 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ElementalActivationsReadOnlyAccess

`ElementalActivationsReadOnlyAccess`adalah kebijakanAWS terkelola yang: Akses hanya-baca ke daftar terperinci aset yang dibeliAkun AWS yang terkait dengan pengguna

Menggunakan kebijakan ini

Anda dapat melampirkan`ElementalActivationsReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 28 Agustus 2020, 16:51 UTC
- Waktu yang telah diedit: 28 Agustus 2020 16.51 UTC

- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

ElementalAppliancesSoftwareFullAccess

`ElementalAppliancesSoftwareFullAccess`adalah kebijakanAWS terkelola yang: Akses penuh untuk melihat dan mengambil tindakan pada kutipan dan pesanan Peralatan Elemental dan Perangkat Lunak

Menggunakan kebijakan ini

Anda dapat melampirkan`ElementalAppliancesSoftwareFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 31 Juli 2019, 16:28 UTC
- Waktu yang telah diedit: 05 Februari 2021 21.01 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ElementalAppliancesSoftwareReadOnlyAccess

`ElementalAppliancesSoftwareReadOnlyAccess`adalah kebijakanAWS terkelola yang: Akses hanya-baca untuk melihat kutipan dan pesanan Peralatan Elemental dan Perangkat Lunak

Menggunakan kebijakan ini

Anda dapat melampirkan`ElementalAppliancesSoftwareReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 01 April 2020, 22:31 UTC
- Waktu yang telah diedit: 01 April 2020, 22.31 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "elemental-appliances-software:List*",
        "elemental-appliances-software:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

ElementalSupportCenterFullAccess

`ElementalSupportCenterFullAccess`adalah kebijakanAWS terkelola yang: Akses penuh untuk melihat dan mengambil tindakan terhadap kasus dukungan Elemental Appliance dan Software dan konten dukungan produk

Menggunakan kebijakan ini

Anda dapat melampirkan`ElementalSupportCenterFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 25 November 2020, 18:08 UTC
- Waktu yang telah diedit: 05 Februari 2021 09.02 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

EMRDescribeClusterPolicyForEMRWAL

`EMRDescribeClusterPolicyForEMRWAL`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin hanya-baca yang memungkinkan layanan WAL untuk Amazon EMR menemukan dan mengembalikan status klaster

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 15 Juni 2023, 23:30 UTC
- Waktu yang telah diedit: 15 Juni 2023, 23.30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

FMSServiceRolePolicy

`FMSServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan akses untuk memungkinkan layanan FM terkait peran untuk melakukan tindakan terkait FM pada sumber daya yang dikelola FM dalam akunAWS Organisasi pelanggan.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

detail kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 28 Maret 2018, 23:01 UTC
- Waktu yang telah diedit: 21 April 2023, 18.33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v28 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "waf:UpdateWebACL",
        "waf:DeleteWebACL",
        "waf:GetWebACL",
        "waf:GetRuleGroup",
        "waf:ListSubscribedRuleGroups",
```

```
        "waf-regional:UpdateWebACL",
        "waf-regional:DeleteWebACL",
        "waf-regional:GetWebACL",
        "waf-regional:GetRuleGroup",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:AssociateWebACL",
        "waf-regional:DisassociateWebACL",
        "elasticloadbalancing:SetWebACL",
        "apigateway:SetWebACL",
        "elasticloadbalancing:SetSecurityGroups",
        "waf:ListTagsForResource",
        "waf-regional:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListLoggingConfigurations",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/webacl/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "waf:CreateWebACL",
        "waf-regional:CreateWebACL",
        "waf:GetChangeToken",
        "waf-regional:GetChangeToken",
        "waf-regional:GetWebACLForResource"
```

```
      ],
      "Resource" : [
        "arn:aws:waf:*:*:*",
        "arn:aws:waf-regional:*:*:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "waf:PutPermissionPolicy",
        "waf:GetPermissionPolicy",
        "waf:DeletePermissionPolicy",
        "waf-regional:PutPermissionPolicy",
        "waf-regional:GetPermissionPolicy",
        "waf-regional:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:rulegroup/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "cloudfront:UpdateDistribution",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListDistributions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "config:DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:StartConfigRulesEvaluation"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/fms.amazonaws.com/
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutConfigurationRecorder",
        "config:StartConfigurationRecorder",
        "config:PutDeliveryChannel",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetComplianceSummaryByConfigRule",
        "config:GetDiscoveredResourceCounts",
        "config:PutEvaluations",
        "config:SelectResourceConfig"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/fms.amazonaws.com/AWSServiceRoleForFMS"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "organizations:ListAccounts",
```

```
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:CreateProtection",
        "shield:DeleteProtection",
        "shield:DescribeProtection",
        "shield:ListProtections",
        "shield:ListAttacks",
        "shield:CreateSubscription",
        "shield:DescribeSubscription",
        "shield:GetSubscriptionState",
        "shield:DescribeDRTAccess",
        "shield:DescribeEmergencyContactSettings",
        "shield:UpdateEmergencyContactSettings",
        "elasticloadbalancing:DescribeLoadBalancers",
        "ec2:DescribeAddresses",
        "shield:EnableApplicationLayerAutomaticResponse",
        "shield:DisableApplicationLayerAutomaticResponse",
        "shield:UpdateApplicationLayerAutomaticResponse"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/FMManaged" : "*"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcPeeringConnections"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:TagResource",
        "wafv2:ListResourcesForWebACL",
        "wafv2:AssociateWebACL",
        "wafv2:ListTagsForResource",
        "wafv2:UntagResource",
        "wafv2:GetWebACL",
        "wafv2:DisassociateFirewallManager",
        "wafv2:DeleteWebACL",
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:UpdateWebACL",
        "wafv2:CreateWebACL",
        "wafv2:DeleteFirewallManagerRuleGroups",
        "wafv2:PutFirewallManagerRuleGroups"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*",
```

```
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/ipset/*",
        "arn:aws:wafv2:*:*:regional/ipset/*",
        "arn:aws:wafv2:*:*:global/regexpatternset/*",
        "arn:aws:wafv2:*:*:regional/regexpatternset/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutPermissionPolicy",
        "wafv2:GetPermissionPolicy",
        "wafv2:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACLForResource"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:CreateAction" : "CreateRouteTable"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "ec2:DeleteRouteTable",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DisassociateRouteTable",
        "ec2:ReplaceRouteTableAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:resource-share/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
```

```
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ram:CreateResourceShare",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Sid" : "ram",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
```

```
            "network-firewall.amazonaws.com",
            "shield.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:AssociateSubnets",
        "network-firewall:CreateFirewall",
        "network-firewall:CreateFirewallPolicy",
        "network-firewall:DisassociateSubnets",
        "network-firewall:UpdateFirewallDeleteProtection",
        "network-firewall:UpdateFirewallPolicy",
        "network-firewall:UpdateFirewallPolicyChangeProtection",
        "network-firewall:UpdateSubnetChangeProtection",
        "network-firewall:AssociateFirewallPolicy",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
```

```
        "network-firewall:PutResourcePolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DeleteResourcePolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:UpdateLoggingConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DeleteFirewallPolicy",
        "network-firewall:DeleteFirewall"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListTagsForResource",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupPolicy",
        "route53resolver:PutFirewallRuleGroupPolicy"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:UpdateFirewallRuleGroupAssociation",
        "route53resolver:DisassociateFirewallRuleGroup"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:AssociateFirewallRuleGroup",
        "route53resolver:TagResource"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

FSxDeleteServiceLinkedRoleAccess

`FSxDeleteServiceLinkedRoleAccess`adalah kebijakanAWS terkelola yang: Memungkinkan Amazon FSx menghapus Peran Tertaut Layanan untuk akses Amazon S3

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 28 November 2018, 10:40 UTC
- Waktu yang telah diedit: 28 November 2018 10.40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetRole"
      ],
      "Resource" : "arn:*:iam::*:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

GameLiftGameServerGroupPolicy

`GameLiftGameServerGroupPolicy`adalah kebijakanAWS terkelola yang: Kebijakan untuk memungkinkan Gamelift GameServerGroups mengelola sumber daya pelanggan

Menggunakan kebijakan ini

Anda dapat melampirkan`GameLiftGameServerGroupPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 03 April 2020, 23:12 UTC
- Waktu yang telah diedit: 13 Mei 2020, 17.27 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/GameLift" : "GameServerGroups"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:EnterStandby",
        "autoscaling:SetInstanceProtection",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:SuspendProcesses",
        "autoscaling:DetachInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/GameLift" : "GameServerGroups"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sns:Publish",
      "Resource" : [
        "arn:*:sns:*:*:ActivatingLifecycleHookTopic-*",
        "arn:*:sns:*:*:TerminatingLifecycleHookTopic-*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/GameLift"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

GlobalAcceleratorFullAccess

`GlobalAcceleratorFullAccess`adalah kebijakanAWS terkelola yang: Izinkan GlobalAccelerator Pengguna Akses penuh ke semua API

Menggunakan kebijakan ini

Anda dapat melampirkan`GlobalAcceleratorFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 November 2018, 02:44 UTC
- Waktu yang telah diedit: 04 Desember 2020, 19.17 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRegions",
        "ec2:DescribeSubnets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "globalaccelerator.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

GlobalAcceleratorReadOnlyAccess

`GlobalAcceleratorReadOnlyAccess`adalah kebijakanAWS terkelola yang: Izinkan GlobalAccelerator Pengguna Mengakses ke API Hanya Baca

Menggunakan kebijakan ini

Anda dapat melampirkan`GlobalAcceleratorReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 November 2018, 02:41 UTC
- Waktu yang telah diedit: 27 November 2018 02.41 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:Describe*",
        "globalaccelerator:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

GreengrassOTAUpdateArtifactAccess

`GreengrassOTAUpdateArtifactAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca ke artefak Pembaruan OTA Greengrass di semua wilayah Greengrass

Menggunakan kebijakan ini

Anda dapat melampirkan`GreengrassOTAUpdateArtifactAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 29 November 2017, 18:11 UTC
- Waktu yang telah diedit: 18 Desember 2018, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

GroundTruthSyntheticConsoleFullAccess

`GroundTruthSyntheticConsoleFullAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin yang diperlukan untuk menggunakan semua fitur SageMaker Ground Truth Synthetic Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`GroundTruthSyntheticConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 25 Agustus 2022, 15:58 UTC
- Waktu yang telah diedit: 25 Agustus 2022 15.58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

GroundTruthSyntheticConsoleReadOnlyAccess

`GroundTruthSyntheticConsoleReadOnlyAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan akses hanya-baca ke SageMaker Ground Truth Synthetic melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`GroundTruthSyntheticConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 25 Agustus 2022, 15:58 UTC
- Waktu yang telah diedit: 25 Agustus 2022, 15.58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

Health_OrganizationsServiceRolePolicy

`Health_OrganizationsServiceRolePolicy`adalah kebijakan AWS terkelola yang: Kebijakan AWS kesehatan untuk mengaktifkan fitur Tampilan Organisasi

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 16 Desember 2019, 13:28 UTC
- Waktu telah diedit: 06 Februari 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

IAMAccessAdvisorReadOnly

`IAMAccessAdvisorReadOnly`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan akses untuk membaca semua informasi akses yang disediakan oleh penasihat akses IAM seperti layanan informasi terakhir diakses.

Menggunakan kebijakan ini

Anda dapat melampirkan`IAMAccessAdvisorReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 21 Juni 2019, 19:33 UTC
- Waktu yang telah diedit: 21 Juni 2019 19.33 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListPolicies",
```

```
        "iam:ListPoliciesGrantingServiceAccess",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GenerateOrganizationsAccessReport",
        "iam:GenerateCredentialReport",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetailsWithEntities",
        "iam:GetOrganizationsAccessReport",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListPolicies",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan menghapus izin identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

IAMAccessAnalyzerFullAccess

`IAMAccessAnalyzerFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke IAM Access Analyzer

Menggunakan kebijakan ini

Anda dapat melampirkan`IAMAccessAnalyzerFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 02 Desember 2019, 17:12 UTC
- Waktu yang telah diedit: 02 Desember 2019 07.12 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "access-analyzer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

IAMAccessAnalyzerReadOnlyAccess

`IAMAccessAnalyzerReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses baca saja ke sumber daya IAM Access Analyzer

Menggunakan kebijakan ini

Anda dapat melampirkan `IAMAccessAnalyzerReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 02 Desember 2019, 17:12 UTC

- Waktu yang telah diedit: 27 November 2023, 02:24 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMAccessAnalyzerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:Get*",
        "access-analyzer:List*",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

IAMFullAccess

`IAMFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke IAM melaluiAWS Management Console.

Menggunakan kebijakan

Anda dapat melampirkan`IAMFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 21 Juni 2019, 19.40 UTC
- ARN: `arn:aws:iam::aws:policy/IAMFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:*",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListChildren",
```

```
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListPolicies",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

IAMReadOnlyAccess

`IAMReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke IAM melaluiAWS Management Console.

Menggunakan kebijakan ini

Anda dapat melampirkan`IAMReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:40 UTC
- Waktu yang telah diedit: 25 Januari 2018 08.08 UTC
- ARN: `arn:aws:iam::aws:policy/IAMReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

IAMSelfManageServiceSpecificCredentials

`IAMSelfManageServiceSpecificCredentials`adalah kebijakanAWS terkelola yang: Memungkinkan pengguna IAM untuk mengelola Kredensi Khusus Layanan mereka sendiri.

Menggunakan kebijakan ini

Anda dapat melampirkan`IAMSelfManageServiceSpecificCredentials` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 22 Desember 2016, 17:25 UTC
- Waktu yang telah diedit: 22 Desember 2016 07.25 UTC
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:ListServiceSpecificCredentials",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus izin identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

IAMUserChangePassword

`IAMUserChangePassword`adalah kebijakanAWS terkelola yang: Memberikan kemampuan bagi pengguna IAM untuk mengubah kata sandi mereka sendiri.

Menggunakan kebijakan ini

Anda dapat melampirkan`IAMUserChangePassword` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 15 November 2016, 00:25 UTC
- Waktu yang telah diedit: 15 November 2016 02.18 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserChangePassword`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

IAMUserSSHKeys

`IAMUserSSHKeys`adalah kebijakanAWS terkelola yang: Menyediakan kemampuan bagi pengguna IAM untuk mengelola kunci SSH mereka sendiri.

Menggunakan kebijakan ini

Anda dapat melampirkan`IAMUserSSHKeys` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola

- Waktu pembuatan: 09 Juli 2015, 17:08 UTC
- Waktu yang telah diedit: 09 Juli 2015 17.08 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserSSHKeys`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan kebijakan

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

IVSFullAccess

`IVSFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke Layanan Video Interaktif (IVS), Juga menyertakan izin untuk layanan dependen, diperlukan untuk akses penuh ke konsol ivs.

Menggunakan kebijakan ini

Anda dapat melampirkan `IVSFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 13 Desember 2023, 21:20 UTC
- Waktu telah diedit: 13 Desember 2023, 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/IVSFullAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:*",
        "ivschat:*"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

IVSReadOnlyAccess

`IVSReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya-baca ke IVS Low-Latency dan Real-Time streaming API

Menggunakan kebijakan ini

Anda dapat melampirkan `IVSReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 05 Desember 2023, 18:00 UTC
- Waktu yang telah diedit: 16 Februari 2024, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/IVSReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "IVSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:BatchGetChannel",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetParticipant",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStageSession",
        "ivs:GetStorageConfiguration",
        "ivs:GetStream",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListParticipants",
        "ivs:ListParticipantEvents",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStageSessions",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin dengan hak istimewa paling sedikit

IVSRecordToS3

`IVSRecordToS3`adalah kebijakanAWS terkelola yang: Peran Tertaut Layanan untuk melakukan S3 PutObject untuk merekam streaming langsung IVS

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 Desember 2020, 00:10 UTC
- Waktu yang telah diedit: 05 Desember 2020, 00:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

KafkaConnectServiceRolePolicy

`KafkaConnectServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin kepada Kafka Connect untuk mengelolaAWS sumber daya atas nama Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan yang melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup grup, grup grup, grup grup, grup, grup, grup, grup, grup, grup,

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 September 2021, 13:12 UTC
- Waktu yang telah diedit: 07 September 2021 13.12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonMSKConnectManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "AmazonMSKConnectManaged"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonMSKConnectManaged" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

KafkaServiceRolePolicy

`KafkaServiceRolePolicy`adalah kebijakanAWS terkelola yang: layanan IAM terkait kebijakan peran untuk Kafka.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran ini.

Detail

- Tipe: Kebijakan peran terkait layanan

- Waktu pembuatan: 15 November 2018, 23:31 UTC
- Waktu yang telah diedit: 28 April 2023, 00:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default adalah versi yang menentukan izin untuk kebijakan ini adalah versi yang menentukan izin untuk kebijakan ini. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AttachNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeVpcEndpoints",
        "acm-pca:GetCertificateAuthorityCertificate",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:*:ec2:*:*:subnet/*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "ec2:ResourceTag/ClusterArn" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "secretsmanager:SecretId" : "arn:*:secretsmanager:*:*:secret:AmazonMSK_*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

KeyspacesReplicationServiceRolePolicy

`KeyspacesReplicationServiceRolePolicy`adalah kebijakanAWS terkelola yang: Izin yang diperlukan oleh Keyspaces untuk replikasi data lintas wilayah

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, grup, atau peran ini.

Rincian kebijakan kebijakan kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 02 Mei 2023, 16:15 UTC
- Waktu yang telah diedit: 02 Mei 2023, 16.15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi default kebijakan yang menentukan izin untuk kebijakan default kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:SelectMultiRegionResource",
        "cassandra:Modify",
```

```
        "cassandra:ModifyMultiRegionResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

LakeFormationDataAccessServiceRolePolicy

`LakeFormationDataAccessServiceRolePolicy`adalah kebijakan AWS terkelola yang: Kebijakan untuk memberikan akses data sementara ke sumber daya Lake Formation

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 20 Juni 2019, 20:46 UTC
- Waktu telah diedit: 06 Februari 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

LexBotPolicy

`LexBotPolicy`adalah kebijakanAWS terkelola yang: Kebijakan untuk kasus penggunaanAWS Lex Bot

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau Anda.

Kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 Februari 2017, 22:18 UTC
- Waktu yang telah diedit: 13 November 2019 08.29 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Kebijakan ini adalah versi yang menentukan kebijakan yang mengizinkan untuk kebijakan yang tidak dapat dilampirkan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectSentiment"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

LexChannelPolicy

`LexChannelPolicy`adalah kebijakanAWS terkelola yang: Kebijakan untuk kasus penggunaanAWS Lex Channel

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, peran, peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 Februari 2017, 23:23 UTC
- Waktu yang telah diedit: 17 Pebruari 2017 05.23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Kebijakan ini adalah versi yang menentukan izin untuk kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen dokumen dokumen dokumen dokumen dokumen dokumen dokumen dokumen dokumen dokumen

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lex:PostText"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

LightsailExportAccess

`LightsailExportAccess`adalah kebijakanAWS terkelola yang: Kebijakan peran terkait layananAWS Lightsail yang memberikan izin untuk mengekspor sumber daya

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 28 September 2018, 16:35 UTC
- Waktu yang telah diedit: 15 Januari 2022, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot",
        "ec2:DescribeSnapshots",
        "ec2:CopyImage",
        "ec2:DescribeImages"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccountPublicAccessBlock"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

MediaConnectGatewayInstanceRolePolicy

`MediaConnectGatewayInstanceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin untuk mendaftarkan Instans MediaConnect Gateway ke MediaConnect Gateway.

Menggunakan kebijakan ini

Anda dapat melampirkan`MediaConnectGatewayInstanceRolePolicy` ke pengguna, grup, dan peran Anda.

Rincian

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 22 Maret 2023, 20:43 UTC
- Waktu yang telah diedit: 22 Maret 2023, 20.43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:PollGateway",
        "mediaconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

MediaPackageServiceRolePolicy

`MediaPackageServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan MediaPackage untuk mempublikasikan log ke CloudWatch

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 September 2020, 17:45 UTC
- Waktu yang telah diedit: 18 September 2020 17.45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/MediaPackage/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/MediaPackage/*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

MemoryDBServiceRolePolicy

`MemoryDBServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini memungkinkan MemoryDB untuk mengelolaAWS sumber daya atas nama Anda sebagaimana diperlukan untuk mengelola sumber daya Anda.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan terkait layanan yang mengizinkan layanan terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan pada pengguna, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 17 Agustus 2021, 22:34 UTC
- Waktu yang telah diedit: 18 Agustus 2021 23.48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonMemoryDBManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonMemoryDBManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/MemoryDB"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

MigrationHubDMSAccessServiceRolePolicy

`MigrationHubDMSAccessServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan untuk Database Migration Service untuk mengambil peran dalam akun pelanggan untuk memanggil Migration Hub

Menggunakan

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan pada,,,,,,,,,,,,,,,,,,,,,,,,

Detail

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan
- Waktu yang telah diedit: 07 Oktober 2019 17.57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgh:CreateProgressUpdateStream",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:DescribeMigrationTask",
        "mgh:AssociateDiscoveredResource",
        "mgh:ListDiscoveredResources",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:DisassociateDiscoveredResource",
        "mgh:AssociateCreatedArtifact",
        "mgh:NotifyMigrationTaskState",
        "mgh:DisassociateCreatedArtifact",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS/migrationTask/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

MigrationHubServiceRolePolicy

`MigrationHubServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Migration Hub untuk memanggil Application Discovery Service atas nama Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup, grup

Detail kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Juni 2019
- Waktu yang telah diedit: 06 Agustus 2020, 18.08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "dms:AddTagsToResource",
      "Resource" : [
        "arn:aws:dms:*:*:endpoint:*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "*"
      ]
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

MigrationHubSMSAccessServiceRolePolicy

`MigrationHubSMSAccessServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan untuk Layanan Migrasi Server untuk mengambil peran dalam akun pelanggan untuk memanggil Migration Hub

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, grup, peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Juni 2019, 18:30 UTC
- Waktu yang telah diedit: 07 Oktober 2019 18.02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgh:CreateProgressUpdateStream",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:DescribeMigrationTask",
        "mgh:AssociateDiscoveredResource",
        "mgh:ListDiscoveredResources",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:DisassociateDiscoveredResource",
        "mgh:AssociateCreatedArtifact",
        "mgh:NotifyMigrationTaskState",
        "mgh:DisassociateCreatedArtifact",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS/migrationTask/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM

- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

MonitronServiceRolePolicy

`MonitronServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan untuk layananAWS Monitron terkait peran pemberian akses ke sumber daya pelanggan yang diperlukan.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran tidak dapat dilampirkan kebijakan ini ke pengguna, atau peran baru.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 02 Mei 2022, 19:22 UTC
- Waktu yang telah diedit: 02 Mei 2022, 19.22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
```

```
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

NeptuneConsoleFullAccess

`NeptuneConsoleFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh untuk mengelola Amazon Neptunus menggunakan. AWS Management Console Perhatikan kebijakan ini juga memberikan akses penuh untuk mempublikasikan semua topik SNS dalam akun, izin untuk membuat dan mengedit instans Amazon EC2 dan konfigurasi VPC, izin untuk melihat dan mencantumkan kunci di Amazon KMS, dan akses penuh ke Amazon RDS. Untuk informasi lebih lanjut, lihat https://aws.amazon.com/neptune/faqs/.

Menggunakan kebijakan ini

Anda dapat melampirkan `NeptuneConsoleFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 19 Juni 2018, 21:35 UTC
- Waktu telah diedit: November 30, 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
            "neptune"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForRDS",
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
```

```
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
```

```
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowOtherDepedentPermissions",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
```

```
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "iam:ListRoles",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForNeptune",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "rds.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "AllowCreateSLRForNeptune",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForNeptuneAnalytics",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:CreateGraph",
        "neptune-graph:DeleteGraph",
        "neptune-graph:GetGraph",
        "neptune-graph:ListGraphs",
        "neptune-graph:UpdateGraph",
        "neptune-graph:ResetGraph",
        "neptune-graph:CreateGraphSnapshot",
        "neptune-graph:DeleteGraphSnapshot",
        "neptune-graph:GetGraphSnapshot",
        "neptune-graph:ListGraphSnapshots",
        "neptune-graph:RestoreGraphFromSnapshot",
        "neptune-graph:CreatePrivateGraphEndpoint",
        "neptune-graph:GetPrivateGraphEndpoint",
        "neptune-graph:ListPrivateGraphEndpoints",
        "neptune-graph:DeletePrivateGraphEndpoint",
        "neptune-graph:CreateGraphUsingImportTask",
        "neptune-graph:GetImportTask",
        "neptune-graph:ListImportTasks",
        "neptune-graph:CancelImportTask"
      ],
      "Resource" : [
        "arn:aws:neptune-graph:*:*:*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForNeptuneAnalytics",
```

```
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "neptune-graph.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateSLRForNeptuneAnalytics",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "neptune-graph.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

NeptuneFullAccess

`NeptuneFullAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke Amazon Neptunus. Perhatikan kebijakan ini juga memberikan akses penuh untuk mempublikasikan semua topik SNS dalam akun dan akses penuh ke Amazon RDS. Untuk informasi lebih lanjut, lihat https://aws.amazon.com/neptune/faqs/.

Menggunakan kebijakan ini

Anda dapat melampirkan `NeptuneFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Mei 2018, 19:17 UTC
- Waktu telah diedit: 22 Januari 2024, 16:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
            "neptune"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBClusterEndpoint",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:CreateGlobalCluster",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterEndpoint",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DeleteGlobalCluster",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
```

```
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:FailoverGlobalCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterEndpoint",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:ModifyGlobalCluster",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveFromGlobalCluster",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime",
        "rds:StartDBCluster",
        "rds:StopDBCluster"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowOtherDepedentPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForNeptune",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateSLRForNeptune",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "AllowDataAccessForNeptune",
      "Effect" : "Allow",
      "Action" : [
        "neptune-db:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

NeptuneGraphReadOnlyAccess

`NeptuneGraphReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya baca ke semua sumber daya Amazon Neptunus Analytics bersama dengan izin baca saja untuk layanan dependen.

Menggunakan kebijakan ini

Anda dapat melampirkan `NeptuneGraphReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 November 2023, 07:32 UTC
- Waktu telah diedit: November 30, 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyPermissionsForNeptuneGraph",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:Get*",
        "neptune-graph:List*",
        "neptune-graph:Read*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForCloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

NeptuneReadOnlyAccess

`NeptuneReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses baca saja ke Amazon Neptunus. Perhatikan bahwa kebijakan ini juga memberikan akses ke sumber daya Amazon RDS. Untuk informasi lebih lanjut, lihat https://aws.amazon.com/neptune/faqs/.

Menggunakan kebijakan ini

Anda dapat melampirkan `NeptuneReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 30 Mei 2018, 19:16 UTC
- Waktu telah diedit: 22 Januari 2024, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyPermissionsForRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
```

```
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForCloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "kms:ListAliases",
        "kms:ListKeyPolicies"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForNeptuneDB",
      "Effect" : "Allow",
      "Action" : [
        "neptune-db:Read*",
        "neptune-db:Get*",
        "neptune-db:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

NetworkAdministrator

`NetworkAdministrator`adalah kebijakanAWS terkelola yang: Memberikan izin akses penuh keAWS layanan dan tindakan yang diperlukan untuk menyiapkan dan mengonfigurasi sumber dayaAWS jaringan.

Menggunakan kebijakan ini

Anda dapat melampirkan`NetworkAdministrator` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan fungsi Job
- Waktu pembuatan: 10 November 2016, 17:31 UTC
- Waktu yang telah diedit: 16 September 2021 20.22 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/NetworkAdministrator`

Versi kebijakan

Versi kebijakan:v11 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudfront:ListDistributions",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "directconnect:*",
```

```
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:CreateCarrierGateway",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateFlowLogs",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpointConnectionNotification",
        "ec2:CreateVpcEndpointServiceConfiguration",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteCarrierGateway",
        "ec2:DeleteEgressOnlyInternetGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
```

```
        "ec2:DeletePlacementGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpointConnectionNotifications",
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
```

```
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeIpv6Pools",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySecurityGroupRules",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ModifyVpcEndpointConnectionNotification",
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:ModifyVpcPeeringConnectionOptions",
        "ec2:ModifyVpcTenancy",
        "ec2:MoveAddressToVpc",
        "ec2:RejectVpcEndpointConnections",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:ResetNetworkInterfaceAttribute",
        "ec2:RestoreAddressToClassic",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
```

```
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticloadbalancing:*",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "route53:*",
        "route53domains:*",
        "sns:CreateTopic",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AttachClassicLinkVpc",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVpcPeeringConnection",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DetachClassicLinkVpc",
        "ec2:DisableVpcClassicLink",
        "ec2:EnableVpcClassicLink",
        "ec2:GetConsoleScreenshot",
        "ec2:RejectVpcPeeringConnection",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLocalGatewayRoute",
        "ec2:CreateLocalGatewayRouteTableVpcAssociation",
        "ec2:DeleteLocalGatewayRoute",
        "ec2:DeleteLocalGatewayRouteTableVpcAssociation",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLocalGateways",
        "ec2:SearchLocalGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "s3:ListBucket"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/flow-logs-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptTransitGatewayVpcAttachment",
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:CreateTransitGateway",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:DeleteTransitGateway",
        "ec2:DeleteTransitGatewayRoute",
        "ec2:DeleteTransitGatewayRouteTable",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DisableTransitGatewayRouteTablePropagation",
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:ExportTransitGatewayRoutes",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:ModifyTransitGateway",
        "ec2:ModifyTransitGatewayVpcAttachment",
        "ec2:RejectTransitGatewayVpcAttachment",
        "ec2:ReplaceTransitGatewayRoute",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "transitgateway.amazonaws.com"
          ]
        }
```

```
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

OAMFullAccess

`OAMFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke CloudWatch Pengamatan Access Manager

Menggunakan kebijakan

Anda dapat melampirkan`OAMFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 November 2022, 13:38 UTC
- Waktu yang telah diedit: 27 November 2022, 13.38 UTC
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

OAMReadOnlyAccess

`OAMReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses Read Only ke CloudWatch Pengamatan Access Manager

Menggunakan kebijakan ini

Anda dapat melampirkan`OAMReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 November 2022, 13:29 UTC
- Waktu yang telah diedit: 27 November 2022, 13.29 UTC
- ARN: `arn:aws:iam::aws:policy/OAMReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:Get*",
        "oam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

PartnerCentralAccountManagementUserRoleAssociation

`PartnerCentralAccountManagementUserRoleAssociation`adalah kebijakan AWS terkelola yang: Menyediakan akses untuk mengaitkan dan memisahkan pengguna pusat mitra dengan peran IAM

Menggunakan kebijakan ini

Anda dapat melampirkan `PartnerCentralAccountManagementUserRoleAssociation` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 10 November 2023, 02:03 UTC
- Waktu telah diedit: 10 November 2023, 02:03 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PassPartnerCentralRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/PartnerCentralRoleFor*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "partnercentral-account-management.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "PartnerUserRoleAssociation",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "partnercentral-account-management:AssociatePartnerUser",
        "partnercentral-account-management:DisassociatePartnerUser"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

PowerUserAccess

`PowerUserAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses penuh ke AWS layanan dan sumber daya, tetapi tidak mengizinkan pengelolaan Pengguna dan grup.

Menggunakan kebijakan ini

Anda dapat melampirkan `PowerUserAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu yang telah diedit: 06 Juli 2023, 22.04 UTC
- ARN: `arn:aws:iam::aws:policy/PowerUserAccess`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "NotAction" : [
        "iam:*",
        "organizations:*",
        "account:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole",
        "iam:DeleteServiceLinkedRole",
        "iam:ListRoles",
        "organizations:DescribeOrganization",
        "account:ListRegions",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling sedikit hak istimewa

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

`QuickSightAccessForS3StorageManagementAnalyticsReadOnly`adalah kebijakanAWS terkelola yang: Kebijakan yang digunakan oleh QuickSight tim untuk mengakses data pelanggan yang dihasilkan oleh S3 Storage Management Analytics.

Menggunakan kebijakan ini

Anda dapat melampirkan`QuickSightAccessForS3StorageManagementAnalyticsReadOnly` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 12 Juni 2017, 18:18 UTC
- Waktu yang telah diedit: 08 Oktober 2019 23.53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::s3-analytics-export-shared-*"
      ]
    },
    {
      "Action" : [
        "s3:GetAnalyticsConfiguration",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

RDSCloudHsmAuthorizationRole

`RDSCloudHsmAuthorizationRole`adalah kebijakanAWS terkelola yang: Kebijakan default untuk peran layanan Amazon RDS.

Menggunakan kebijakan ini

Anda dapat melampirkan`RDSCloudHsmAuthorizationRole` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 26 September 2019 08.14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm:DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ReadOnlyAccess

`ReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya-baca ke AWS layanan dan sumber daya.

Menggunakan kebijakan ini

Anda dapat melampirkan `ReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu telah diedit: 05 Februari 2024, 15:00 UTC
- ARN: `arn:aws:iam::aws:policy/ReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v111 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "a4b:Get*",
        "a4b:List*",
        "a4b:Search*",
        "access-analyzer:GetAccessPreview",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
```

```
        "access-analyzer:GetFinding",
        "access-analyzer:GetGeneratedPolicy",
        "access-analyzer:ListAccessPreviewFindings",
        "access-analyzer:ListAccessPreviews",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListPolicyGenerations",
        "access-analyzer:ListTagsForResource",
        "access-analyzer:ValidatePolicy",
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetChallengeQuestions",
        "account:GetContactInformation",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "acm-pca:Describe*",
        "acm-pca:Get*",
        "acm-pca:List*",
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:GetJob",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListJobs",
        "aoss:BatchGetCollection",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetAccountSettings",
        "aoss:GetPoliciesStats",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollections",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
```

```
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "apigateway:GET",
        "appconfig:GetApplication",
        "appconfig:GetConfiguration",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appfabric:GetAppAuthorization",
        "appfabric:GetAppBundle",
        "appfabric:GetIngestion",
        "appfabric:GetIngestionDestination",
        "appfabric:ListAppAuthorizations",
        "appfabric:ListAppBundles",
        "appfabric:ListIngestionDestinations",
        "appfabric:ListIngestions",
        "appfabric:ListTagsForResource",
        "appflow:DescribeConnector",
        "appflow:DescribeConnectorEntity",
        "appflow:DescribeConnectorFields",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeConnectors",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecution",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:DescribeFlows",
        "appflow:ListConnectorEntities",
        "appflow:ListConnectorFields",
        "appflow:ListConnectors",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "application-autoscaling:ListTagsForResource",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
```

```
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appstream:Describe*",
        "appstream:List*",
        "appsync:Get*",
        "appsync:List*",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeWorkspace",
        "aps:GetAlertManagerSilence",
        "aps:GetAlertManagerStatus",
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:ListAlertManagerAlertGroups",
        "aps:ListAlertManagerAlerts",
        "aps:ListAlertManagerReceivers",
        "aps:ListAlertManagerSilences",
        "aps:ListAlerts",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListRules",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "aps:QueryMetrics",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:ListAutoshifts",
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts",
        "artifact:GetReport",
```

```
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports",
        "athena:Batch*",
        "athena:Get*",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:GetAssessmentFramework",
        "auditmanager:GetAssessmentReportUrl",
        "auditmanager:GetChangeLogs",
        "auditmanager:GetControl",
        "auditmanager:GetDelegations",
        "auditmanager:GetEvidence",
        "auditmanager:GetEvidenceByEvidenceFolder",
        "auditmanager:GetEvidenceFolder",
        "auditmanager:GetEvidenceFoldersByAssessment",
        "auditmanager:GetEvidenceFoldersByAssessmentControl",
        "auditmanager:GetOrganizationAdminAccount",
        "auditmanager:GetServicesInScope",
        "auditmanager:GetSettings",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListAssessments",
        "auditmanager:ListControls",
        "auditmanager:ListKeywordsForDataSource",
        "auditmanager:ListNotifications",
        "auditmanager:ListTagsForResource",
        "auditmanager:ValidateAssessmentReportIntegrity",
        "autoscaling-plans:Describe*",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:Describe*",
        "autoscaling:GetPredictiveScalingForecast",
        "aws-portal:View*",
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway",
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings",
        "backup-gateway:GetVirtualMachine",
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:Describe*",
```

```
        "backup:Get*",
        "backup:List*",
        "batch:Describe*",
        "batch:List*",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:GetCustomModel",
        "bedrock:GetDataSource",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetIngestionJob",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:GetUseCaseForModelAccess",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAgentVersions",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
        "bedrock:ListFoundationModelAgreementOffers",
        "bedrock:ListFoundationModels",
        "bedrock:ListIngestionJobs",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:ListProvisionedModelThroughputs",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billingconductor:GetBillingGroupCostReport",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroupCostReports",
```

```
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListCustomLineItemVersions",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingPlansAssociatedWithPricingRule",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListResourcesAssociatedToCustomLineItem",
        "billingconductor:ListTagsForResource",
        "braket:GetDevice",
        "braket:GetJob",
        "braket:GetQuantumTask",
        "braket:SearchDevices",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "budgets:Describe*",
        "budgets:View*",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:DescribeNotificationSubscription",
        "ce:DescribeReport",
        "ce:GetAnomalies",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:GetApproximateUsageRecords",
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageWithResources",
        "ce:GetCostCategories",
        "ce:GetCostForecast",
        "ce:GetDimensionValues",
        "ce:GetPreferences",
        "ce:GetReservationCoverage",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetReservationUtilization",
        "ce:GetRightsizingRecommendation",
        "ce:GetSavingsPlanPurchaseRecommendationDetails",
        "ce:GetSavingsPlansCoverage",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "ce:GetSavingsPlansUtilization",
        "ce:GetSavingsPlansUtilizationDetails",
        "ce:GetTags",
        "ce:GetUsageForecast",
        "ce:ListCostAllocationTags",
        "ce:ListCostCategoryDefinitions",
```

```
        "ce:ListSavingsPlansPurchaseRecommendationGeneration",
        "ce:ListTagsForResource",
        "chatbot:Describe*",
        "chatbot:Get*",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chatbot:ListMicrosoftTeamsConfiguredTeams",
        "chatbot:ListMicrosoftTeamsUserIdentities",
        "chime:Get*",
        "chime:List*",
        "chime:Retrieve*",
        "chime:Search*",
        "chime:Validate*",
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource",
        "cloud9:Describe*",
        "cloud9:List*",
        "clouddirectory:BatchRead",
        "clouddirectory:Get*",
        "clouddirectory:List*",
        "clouddirectory:LookupPolicy",
        "cloudformation:Describe*",
        "cloudformation:Detect*",
        "cloudformation:Estimate*",
        "cloudformation:Get*",
```

```
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudhsm:Describe*",
        "cloudhsm:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:Describe*",
        "cloudtrail:Get*",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackage",
        "codeartifact:DescribePackageVersion",
        "codeartifact:DescribeRepository",
        "codeartifact:GetAuthorizationToken",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetPackageVersionAsset",
        "codeartifact:GetPackageVersionReadme",
        "codeartifact:GetRepositoryEndpoint",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersionAssets",
        "codeartifact:ListPackageVersionDependencies",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListRepositoriesInDomain",
        "codeartifact:ListTagsForResource",
        "codeartifact:ReadFromRepository",
        "codebuild:BatchGet*",
        "codebuild:DescribeCodeCoverages",
        "codebuild:DescribeTestCases",
        "codebuild:List*",
        "codecatalyst:GetBillingAuthorization",
```

```
        "codecatalyst:GetConnection",
        "codecatalyst:GetPendingConnection",
        "codecatalyst:ListConnections",
        "codecatalyst:ListIamRolesForConnection",
        "codecatalyst:ListTagsForResource",
        "codecommit:BatchGet*",
        "codecommit:Describe*",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:List*",
        "codedeploy:BatchGet*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:Get*",
        "codeguru-reviewer:List*",
        "codepipeline:Get*",
        "codepipeline:List*",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetRepositorySyncStatus",
        "codestar-connections:GetResourceSyncStatus",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:ListConnections",
        "codestar-connections:ListHosts",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListRepositorySyncDefinitions",
        "codestar-connections:ListSyncConfigurations",
        "codestar-connections:ListTagsForResource",
        "codestar-notifications:describeNotificationRule",
        "codestar-notifications:listEventTypes",
        "codestar-notifications:listNotificationRules",
        "codestar-notifications:listTagsForResource",
        "codestar-notifications:ListTargets",
        "codestar:Describe*",
        "codestar:Get*",
        "codestar:List*",
        "codestar:Verify*",
        "cognito-identity:Describe*",
        "cognito-identity:GetCredentialsForIdentity",
```

```
        "cognito-identity:GetIdentityPoolAnalytics",
        "cognito-identity:GetIdentityPoolDailyAnalytics",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetIdentityProviderDailyAnalytics",
        "cognito-identity:GetOpenIdToken",
        "cognito-identity:GetOpenIdTokenForDeveloperIdentity",
        "cognito-identity:List*",
        "cognito-identity:Lookup*",
        "cognito-idp:AdminGet*",
        "cognito-idp:AdminList*",
        "cognito-idp:Describe*",
        "cognito-idp:Get*",
        "cognito-idp:List*",
        "cognito-sync:Describe*",
        "cognito-sync:Get*",
        "cognito-sync:List*",
        "cognito-sync:QueryRecords",
        "comprehend:BatchDetect*",
        "comprehend:Classify*",
        "comprehend:Contains*",
        "comprehend:Describe*",
        "comprehend:Detect*",
        "comprehend:List*",
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetRecommendationSummaries",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:SelectAggregateResourceConfig",
```

```
        "config:SelectResourceConfig",
        "connect:Describe*",
        "connect:GetContactAttributes",
        "connect:GetCurrentMetricData",
        "connect:GetCurrentUserData",
        "connect:GetFederationToken",
        "connect:GetMetricData",
        "connect:GetMetricDataV2",
        "connect:GetTaskTemplate",
        "connect:GetTrafficDistribution",
        "connect:List*",
        "consoleapp:GetDeviceIdentity",
        "consoleapp:ListDeviceIdentities",
        "consolidatedbilling:GetAccountBillingRole",
        "consolidatedbilling:ListLinkedAccounts",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeJobRun",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobRuns",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "databrew:ListTagsForResource",
        "dataexchange:Get*",
        "dataexchange:List*",
        "datapipeline:Describe*",
```

```
        "datapipeline:EvaluateExpression",
        "datapipeline:Get*",
        "datapipeline:List*",
        "datapipeline:QueryObjects",
        "datapipeline:Validate*",
        "datasync:Describe*",
        "datasync:List*",
        "dax:BatchGetItem",
        "dax:Describe*",
        "dax:GetItem",
        "dax:ListTags",
        "dax:Query",
        "dax:Scan",
        "deepcomposer:GetComposition",
        "deepcomposer:GetModel",
        "deepcomposer:GetSampleModel",
        "deepcomposer:ListCompositions",
        "deepcomposer:ListModels",
        "deepcomposer:ListSampleModels",
        "deepcomposer:ListTrainingTopics",
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:Get*",
        "detective:List*",
        "detective:SearchGraph",
        "devicefarm:Get*",
        "devicefarm:List*",
        "devops-guru:DescribeAccountHealth",
        "devops-guru:DescribeAccountOverview",
        "devops-guru:DescribeAnomaly",
        "devops-guru:DescribeEventSourcesConfig",
        "devops-guru:DescribeFeedback",
        "devops-guru:DescribeInsight",
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationOverview",
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeResourceCollectionHealth",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetCostEstimation",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListAnomaliesForInsight",
        "devops-guru:ListAnomalousLogGroups",
        "devops-guru:ListEvents",
        "devops-guru:ListInsights",
```

```
        "devops-guru:ListMonitoredResources",
        "devops-guru:ListNotificationChannels",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:ListRecommendations",
        "devops-guru:SearchInsights",
        "devops-guru:StartCostEstimation",
        "directconnect:Describe*",
        "discovery:Describe*",
        "discovery:Get*",
        "discovery:List*",
        "dlm:Get*",
        "dms:Describe*",
        "dms:List*",
        "dms:Test*",
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeLaunchConfigurationTemplates",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceNetworks",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListLaunchActions",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "ds:Check*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ds:Verify*",
        "dynamodb:BatchGet*",
        "dynamodb:Describe*",
        "dynamodb:Get*",
        "dynamodb:List*",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "dynamodb:Scan",
        "ec2:Describe*",
        "ec2:Get*",
        "ec2:ListImagesInRecycleBin",
```

```
        "ec2:ListSnapshotsInRecycleBin",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ec2messages:Get*",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetAuthorizationToken",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchCheck*",
        "ecr:BatchGet*",
        "ecr:Describe*",
        "ecr:Get*",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:Describe*",
        "eks:List*",
        "elastic-inference:DescribeAcceleratorOfferings",
        "elastic-inference:DescribeAccelerators",
        "elastic-inference:DescribeAcceleratorTypes",
        "elastic-inference:ListTagsForResource",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:Request*",
        "elasticbeanstalk:Retrieve*",
        "elasticbeanstalk:Validate*",
        "elasticfilesystem:Describe*",
        "elasticfilesystem:ListTagsForResource",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:List*",
        "elasticmapreduce:View*",
        "elastictranscoder:List*",
        "elastictranscoder:Read*",
```

```
        "elemental-appliances-software:Get*",
        "elemental-appliances-software:List*",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "emr-serverless:ListTagsForResource",
        "es:Describe*",
        "es:ESHttpGet",
        "es:ESHttpHead",
        "es:Get*",
        "es:List*",
        "events:Describe*",
        "events:List*",
        "events:Test*",
        "evidently:GetExperiment",
        "evidently:GetExperimentResults",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegmentReferences",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "evidently:TestSegmentPattern",
        "firehose:Describe*",
        "firehose:List*",
        "fis:GetAction",
        "fis:GetExperiment",
        "fis:GetExperimentTargetAccountConfiguration",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
```

```
        "fis:GetTargetResourceType",
        "fis:ListActions",
        "fis:ListExperimentResolvedTargets",
        "fis:ListExperiments",
        "fis:ListExperimentTargetAccountConfigurations",
        "fis:ListExperimentTemplates",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "fis:ListTargetResourceTypes",
        "fms:GetAdminAccount",
        "fms:GetAppsList",
        "fms:GetComplianceDetail",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:GetProtectionStatus",
        "fms:GetProtocolsList",
        "fms:GetViolationDetails",
        "fms:ListAppsLists",
        "fms:ListComplianceStatus",
        "fms:ListMemberAccounts",
        "fms:ListPolicies",
        "fms:ListProtocolsLists",
        "fms:ListTagsForResource",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeExplainability",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribeMonitor",
        "forecast:DescribePredictor",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:DescribeWhatIfAnalysis",
        "forecast:DescribeWhatIfForecast",
        "forecast:DescribeWhatIfForecastExport",
        "forecast:GetAccuracyMetrics",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasetImportJobs",
        "forecast:ListDatasets",
        "forecast:ListExplainabilities",
        "forecast:ListExplainabilityExports",
        "forecast:ListForecastExportJobs",
```

```
        "forecast:ListForecasts",
        "forecast:ListMonitorEvaluations",
        "forecast:ListMonitors",
        "forecast:ListPredictorBacktestExportJobs",
        "forecast:ListPredictors",
        "forecast:ListWhatIfAnalyses",
        "forecast:ListWhatIfForecastExports",
        "forecast:ListWhatIfForecasts",
        "forecast:QueryForecast",
        "forecast:QueryWhatIfForecast",
        "frauddetector:BatchGetVariable",
        "frauddetector:DescribeDetector",
        "frauddetector:DescribeModelVersions",
        "frauddetector:GetBatchImportJobs",
        "frauddetector:GetBatchPredictionJobs",
        "frauddetector:GetDeleteEventsByEventTypeStatus",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEvent",
        "frauddetector:GetEventPredictionMetadata",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetKMSEncryptionKey",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModels",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListEventPredictions",
        "frauddetector:ListTagsForResource",
        "freertos:Describe*",
        "freertos:List*",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:Describe*",
        "gamelift:Get*",
        "gamelift:List*",
        "gamelift:ResolveAlias",
```

```
        "gamelift:Search*",
        "glacier:Describe*",
        "glacier:Get*",
        "glacier:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:BatchGetCrawlers",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetTriggers",
        "glue:BatchGetWorkflows",
        "glue:CheckSchemaVersionValidity",
        "glue:GetCatalogImportStatus",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlerMetrics",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDataflowGraph",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobBookmark",
        "glue:GetJobRun",
        "glue:GetJobRuns",
        "glue:GetJobs",
        "glue:GetMapping",
        "glue:GetMLTaskRun",
        "glue:GetMLTaskRuns",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetPlan",
        "glue:GetRegistry",
        "glue:GetResourcePolicy",
        "glue:GetSchema",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
```

```
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetTriggers",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions",
        "glue:GetWorkflow",
        "glue:GetWorkflowRun",
        "glue:GetWorkflowRunProperties",
        "glue:GetWorkflowRuns",
        "glue:ListCrawlers",
        "glue:ListCrawls",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListSchemas",
        "glue:ListSchemaVersions",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "glue:QuerySchemaVersionMetadata",
        "glue:SearchTables",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListPermissions",
        "grafana:ListTagsForResource",
        "grafana:ListVersions",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:Get*",
        "greengrass:List*",
        "groundstation:DescribeContact",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMinuteUsage",
        "groundstation:GetMissionProfile",
        "groundstation:GetSatellite",
        "groundstation:ListConfigs",
```

```
        "groundstation:ListContacts",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListGroundStations",
        "groundstation:ListMissionProfiles",
        "groundstation:ListSatellites",
        "groundstation:ListTagsForResource",
        "guardduty:Describe*",
        "guardduty:Get*",
        "guardduty:List*",
        "health:Describe*",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRExportJob",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:GetCapabilities",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListFHIRExportJobs",
        "healthlake:ListFHIRImportJobs",
        "healthlake:ListTagsForResource",
        "healthlake:ReadResource",
        "healthlake:SearchWithGet",
        "healthlake:SearchWithPost",
        "iam:Generate*",
        "iam:Get*",
        "iam:List*",
        "iam:Simulate*",
        "identity-sync:GetSyncProfile",
        "identity-sync:GetSyncTarget",
        "identity-sync:ListSyncFilters",
        "identitystore-auth:BatchGetSession",
        "identitystore-auth:ListSessions",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:DescribeUser",
        "identitystore:GetGroupId",
        "identitystore:GetGroupMembershipId",
        "identitystore:GetUserId",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
        "imagebuilder:Get*",
        "imagebuilder:List*",
        "importexport:Get*",
```

```
        "importexport:List*",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListMembers",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
        "iot1click:DescribeDevice",
        "iot1click:DescribePlacement",
        "iot1click:DescribeProject",
        "iot1click:GetDeviceMethods",
        "iot1click:GetDevicesInPlacement",
        "iot1click:ListDeviceEvents",
        "iot1click:ListDevices",
        "iot1click:ListPlacements",
        "iot1click:ListProjects",
        "iot1click:ListTagsForResource",
        "iotanalytics:Describe*",
        "iotanalytics:Get*",
```

```
        "iotanalytics:List*",
        "iotanalytics:SampleChannelData",
        "iotevents:DescribeAlarm",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetector",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:DescribeLoggingOptions",
        "iotevents:ListAlarmModels",
        "iotevents:ListAlarmModelVersions",
        "iotevents:ListAlarms",
        "iotevents:ListDetectorModels",
        "iotevents:ListDetectorModelVersions",
        "iotevents:ListDetectors",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleethub:DescribeApplication",
        "iotfleethub:ListApplications",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetLoggingOptions",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetRegisterAccountStatus",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:GetVehicleStatus",
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListFleetsForVehicle",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotfleetwise:ListVehiclesInFleet",
        "iotroborunner:GetDestination",
        "iotroborunner:GetSite",
        "iotroborunner:GetWorker",
        "iotroborunner:GetWorkerFleet",
```

```
        "iotroborunner:ListDestinations",
        "iotroborunner:ListSites",
        "iotroborunner:ListWorkerFleets",
        "iotroborunner:ListWorkers",
        "iotsitewise:Describe*",
        "iotsitewise:Get*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetEventConfigurationByResourceTypes",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetLogLevelsByResourceTypes",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetMulticastGroupSession",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetPartnerAccount",
        "iotwireless:GetPosition",
        "iotwireless:GetPositionConfiguration",
        "iotwireless:GetPositionEstimate",
        "iotwireless:GetResourceEventConfiguration",
        "iotwireless:GetResourceLogLevel",
        "iotwireless:GetResourcePosition",
        "iotwireless:GetServiceEndpoint",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessDeviceStatistics",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayCertificate",
        "iotwireless:GetWirelessGatewayFirmwareInformation",
        "iotwireless:GetWirelessGatewayStatistics",
        "iotwireless:GetWirelessGatewayTask",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListDevicesForWirelessDeviceImportTask",
        "iotwireless:ListEventConfigurations",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListMulticastGroupsByFuotaTask",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListPartnerAccounts",
        "iotwireless:ListPositionConfigurations",
        "iotwireless:ListQueuedMessages",
```

```
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:BatchGetChannel",
        "ivs:GetChannel",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka:Describe*",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:Get*",
        "kafka:GetBootstrapBrokers",
        "kafka:GetCompatibleKafkaVersions",
        "kafka:List*",
        "kafka:ListClusterOperations",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurationRevisions",
        "kafka:ListConfigurations",
        "kafka:ListKafkaVersions",
        "kafka:ListNodes",
        "kafka:ListTagsForResource",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
```

```
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra:BatchGetDocumentStatus",
        "kendra:DescribeDataSource",
        "kendra:DescribeExperience",
        "kendra:DescribeFaq",
        "kendra:DescribeIndex",
        "kendra:DescribePrincipalMapping",
        "kendra:DescribeQuerySuggestionsBlockList",
        "kendra:DescribeQuerySuggestionsConfig",
        "kendra:DescribeThesaurus",
        "kendra:GetQuerySuggestions",
        "kendra:GetSnapshots",
        "kendra:ListDataSources",
        "kendra:ListDataSourceSyncJobs",
        "kendra:ListEntityPersonas",
        "kendra:ListExperienceEntities",
        "kendra:ListExperiences",
        "kendra:ListFaqs",
        "kendra:ListGroupsOlderThanOrderingId",
        "kendra:ListIndices",
        "kendra:ListQuerySuggestionsBlockLists",
        "kendra:ListTagsForResource",
        "kendra:ListThesauri",
        "kendra:Query",
        "kinesis:Describe*",
        "kinesis:Get*",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:Discover*",
        "kinesisanalytics:Get*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kinesisvideo:Get*",
        "kinesisvideo:List*",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetEffectivePermissionsForPath",
        "lakeformation:GetLfTag",
        "lakeformation:GetResourceLfTags",
```

```
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListLfTags",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListTableStorageOptimizers",
        "lakeformation:SearchDatabasesByLfTags",
        "lakeformation:SearchTablesByLfTags",
        "lambda:Get*",
        "lambda:List*",
        "launchwizard:DescribeAdditionalNode",
        "launchwizard:DescribeProvisionedApp",
        "launchwizard:DescribeProvisioningEvents",
        "launchwizard:DescribeSettingsSet",
        "launchwizard:GetDeployment",
        "launchwizard:GetInfrastructureSuggestion",
        "launchwizard:GetIpAddress",
        "launchwizard:GetResourceCostEstimate",
        "launchwizard:GetResourceRecommendation",
        "launchwizard:GetSettingsSet",
        "launchwizard:GetWorkload",
        "launchwizard:GetWorkloadAsset",
        "launchwizard:GetWorkloadAssets",
        "launchwizard:ListAdditionalNodes",
        "launchwizard:ListAllowedResources",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListProvisionedApps",
        "launchwizard:ListResourceCostEstimates",
        "launchwizard:ListSettingsSets",
        "launchwizard:ListWorkloadDeploymentOptions",
        "launchwizard:ListWorkloadDeploymentPatterns",
        "launchwizard:ListWorkloads",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotChannel",
        "lex:DescribeBotLocale",
        "lex:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
        "lex:Get*",
```

```
        "lex:ListBotAliases",
        "lex:ListBotChannels",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
        "lex:ListImports",
        "lex:ListIntents",
        "lex:ListSlots",
        "lex:ListSlotTypes",
        "lex:ListTagsForResource",
        "license-manager:Get*",
        "license-manager:List*",
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetAutoSnapshots",
        "lightsail:GetBlueprints",
        "lightsail:GetBucketAccessKeys",
        "lightsail:GetBucketBundles",
        "lightsail:GetBucketMetricData",
        "lightsail:GetBuckets",
        "lightsail:GetBundles",
        "lightsail:GetCertificates",
        "lightsail:GetCloudFormationStackRecords",
        "lightsail:GetContainerAPIMetadata",
        "lightsail:GetContainerImages",
        "lightsail:GetContainerServiceDeployments",
        "lightsail:GetContainerServiceMetricData",
        "lightsail:GetContainerServicePowers",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDistributionBundles",
        "lightsail:GetDistributionLatestCacheReset",
        "lightsail:GetDistributionMetricData",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetExportSnapshotRecords",
        "lightsail:GetInstance",
```

```
        "lightsail:GetInstanceMetricData",
        "lightsail:GetInstancePortStates",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstanceState",
        "lightsail:GetKeyPair",
        "lightsail:GetKeyPairs",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancerMetricData",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperation",
        "lightsail:GetOperations",
        "lightsail:GetOperationsForResource",
        "lightsail:GetRegions",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseBlueprints",
        "lightsail:GetRelationalDatabaseBundles",
        "lightsail:GetRelationalDatabaseEvents",
        "lightsail:GetRelationalDatabaseLogEvents",
        "lightsail:GetRelationalDatabaseLogStreams",
        "lightsail:GetRelationalDatabaseMetricData",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "lightsail:Is*",
        "logs:Describe*",
        "logs:FilterLogEvents",
        "logs:Get*",
        "logs:ListAnomalies",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "logs:StartLiveTail",
        "logs:StartQuery",
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "lookoutequipment:DescribeDataIngestionJob",
```

```
        "lookoutequipment:DescribeDataset",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:DescribeLabel",
        "lookoutequipment:DescribeLabelGroup",
        "lookoutequipment:DescribeModel",
        "lookoutequipment:DescribeModelVersion",
        "lookoutequipment:DescribeResourcePolicy",
        "lookoutequipment:DescribeRetrainingScheduler",
        "lookoutequipment:ListDataIngestionJobs",
        "lookoutequipment:ListDatasets",
        "lookoutequipment:ListInferenceEvents",
        "lookoutequipment:ListInferenceExecutions",
        "lookoutequipment:ListInferenceSchedulers",
        "lookoutequipment:ListLabelGroups",
        "lookoutequipment:ListLabels",
        "lookoutequipment:ListModels",
        "lookoutequipment:ListModelVersions",
        "lookoutequipment:ListRetrainingSchedulers",
        "lookoutequipment:ListSensorStatistics",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:Describe*",
        "lookoutmetrics:Get*",
        "lookoutmetrics:List*",
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModelPackagingJobs",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "m2:GetApplication",
        "m2:GetApplicationVersion",
        "m2:GetBatchJobExecution",
        "m2:GetDataSetDetails",
        "m2:GetDataSetImportTask",
        "m2:GetDeployment",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListApplicationVersions",
        "m2:ListBatchJobDefinitions",
        "m2:ListBatchJobExecutions",
        "m2:ListDataSetImportHistory",
```

```
        "m2:ListDataSets",
        "m2:ListDeployments",
        "m2:ListEngineVersions",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:Describe*",
        "machinelearning:Get*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:DescribeBuckets",
        "macie2:DescribeClassificationJob",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAdministratorAccount",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetBucketStatistics",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetClassificationScope",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindings",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetFindingStatistics",
        "macie2:GetInvitationsCount",
        "macie2:GetMacieSession",
        "macie2:GetMember",
        "macie2:GetResourceProfile",
        "macie2:GetRevealConfiguration",
        "macie2:GetSensitiveDataOccurrencesAvailability",
        "macie2:GetSensitivityInspectionTemplate",
        "macie2:GetUsageStatistics",
        "macie2:GetUsageTotals",
        "macie2:ListAllowLists",
        "macie2:ListClassificationJobs",
        "macie2:ListClassificationScopes",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindings",
        "macie2:ListFindingsFilters",
        "macie2:ListInvitations",
        "macie2:ListMembers",
        "macie2:ListOrganizationAdminAccounts",
        "macie2:ListResourceProfileArtifacts",
        "macie2:ListResourceProfileDetections",
        "macie2:ListSensitivityInspectionTemplates",
        "macie2:ListTagsForResource",
```

```
        "macie2:SearchResources",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:GetProposal",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNetworks",
        "managedblockchain:ListNodes",
        "managedblockchain:ListProposals",
        "managedblockchain:ListProposalVotes",
        "managedblockchain:ListTagsForResource",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeOffering",
        "mediaconnect:DescribeReservation",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:ListTagsForResource",
        "mediaconvert:DescribeEndpoints",
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "medialive:DescribeChannel",
        "medialive:DescribeInput",
        "medialive:DescribeInputDevice",
        "medialive:DescribeInputDeviceThumbnail",
        "medialive:DescribeInputSecurityGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeOffering",
        "medialive:DescribeReservation",
        "medialive:DescribeSchedule",
        "medialive:ListChannels",
        "medialive:ListInputDevices",
        "medialive:ListInputDeviceTransfers",
        "medialive:ListInputs",
        "medialive:ListInputSecurityGroups",
        "medialive:ListMultiplexes",
        "medialive:ListMultiplexPrograms",
        "medialive:ListOfferings",
        "medialive:ListReservations",
        "medialive:ListTagsForResource",
        "mediapackage-vod:Describe*",
```

```
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetHeadObject",
        "mediapackagev2:GetObject",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediapackagev2:ListTagsForResource",
        "mediastore:DescribeContainer",
        "mediastore:DescribeObject",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:GetLifecyclePolicy",
        "mediastore:GetMetricPolicy",
        "mediastore:GetObject",
        "mediastore:ListContainers",
        "mediastore:ListItems",
        "mediastore:ListTagsForResource",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:ListTags",
        "mgh:Describe*",
        "mgh:GetHomeRegion",
        "mgh:List*",
        "mgn:DescribeJobLogItems",
        "mgn:DescribeJobs",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:DescribeSourceServers",
        "mgn:DescribeVcenterClients",
        "mgn:GetLaunchConfiguration",
        "mgn:GetReplicationConfiguration",
        "mgn:ListApplications",
        "mgn:ListSourceServerActions",
        "mgn:ListTemplateActions",
        "mgn:ListWaves",
        "mobileanalytics:Get*",
```

```
        "mobiletargeting:Get*",
        "mobiletargeting:List*",
        "monitron:GetProject",
        "monitron:GetProjectAdminUser",
        "monitron:ListProjects",
        "monitron:ListTagsForResource",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnections",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetConnectPeerAssociations",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkChangeEvents",
        "networkmanager:GetCoreNetworkChangeSet",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetNetworkResourceCounts",
        "networkmanager:GetNetworkResourceRelationships",
        "networkmanager:GetNetworkResources",
        "networkmanager:GetNetworkRoutes",
        "networkmanager:GetNetworkTelemetry",
        "networkmanager:GetResourcePolicy",
        "networkmanager:GetRouteAnalysis",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayConnectPeerAssociations",
        "networkmanager:GetTransitGatewayPeering",
```

```
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworkPolicyVersions",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "nimble:GetEula",
        "nimble:GetFeatureMap",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileMember",
        "nimble:GetStreamingImage",
        "nimble:GetStreamingSession",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:GetStudioMember",
        "nimble:ListEulaAcceptances",
        "nimble:ListEulas",
        "nimble:ListLaunchProfileMembers",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStreamingSessions",
        "nimble:ListStudioComponents",
        "nimble:ListStudioMembers",
        "nimble:ListStudios",
        "nimble:ListTagsForResource",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:ListTagsForResource",
        "notifications:GetEventRule",
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:ListTagsForResource",
        "oam:GetLink",
        "oam:GetSink",
```

```
        "oam:GetSinkPolicy",
        "oam:ListAttachedLinks",
        "oam:ListLinks",
        "oam:ListSinks",
        "omics:Get*",
        "omics:List*",
        "one:GetDeviceConfigurationTemplate",
        "one:GetDeviceInstance",
        "one:GetDeviceInstanceConfiguration",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceConfigurationTemplates",
        "one:ListDeviceInstances",
        "one:ListSites",
        "one:ListUsers",
        "opsworks-cm:Describe*",
        "opsworks-cm:List*",
        "opsworks:Describe*",
        "opsworks:Get*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:GetPipelineBlueprint",
        "osis:GetPipelineChangeProgress",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "outposts:Get*",
        "outposts:List*",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:GetPublicKeyCertificate",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentPreferences",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
```

```
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListServicePrincipalNames",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "personalize:Describe*",
        "personalize:Get*",
        "personalize:List*",
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "polly:Describe*",
        "polly:Get*",
        "polly:List*",
        "polly:SynthesizeSpeech",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetPriceListFileUrl",
        "pricing:GetProducts",
        "pricing:ListPriceLists",
        "proton:GetDeployment",
        "proton:GetEnvironment",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:ListDeployments",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplates",
        "proton:ListServiceInstances",
        "proton:ListServices",
        "proton:ListServiceTemplates",
        "proton:ListTagsForResource",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
```

```
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ViewPurchaseOrders",
        "qldb:DescribeJournalKinesisStream",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "qldb:ListTagsForResource",
        "ram:Get*",
        "ram:List*",
        "rbin:GetRule",
        "rbin:ListRules",
        "rbin:ListTagsForResource",
        "rds:Describe*",
        "rds:Download*",
        "rds:List*",
        "redshift:Describe*",
        "redshift:GetReservedNodeExchangeOfferings",
        "redshift:View*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetResourcePolicy",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListEnvironmentVpcs",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:CompareFaces",
        "rekognition:DescribeDataset",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DescribeStreamProcessor",
        "rekognition:Detect*",
        "rekognition:GetCelebrityInfo",
        "rekognition:GetCelebrityRecognition",
        "rekognition:GetContentModeration",
```

```
        "rekognition:GetFaceDetection",
        "rekognition:GetFaceSearch",
        "rekognition:GetLabelDetection",
        "rekognition:GetPersonTracking",
        "rekognition:GetSegmentDetection",
        "rekognition:GetTextDetection",
        "rekognition:List*",
        "rekognition:RecognizeCelebrities",
        "rekognition:Search*",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppAssessment",
        "resiliencehub:DescribeAppVersion",
        "resiliencehub:DescribeAppVersionAppComponent",
        "resiliencehub:DescribeAppVersionResource",
        "resiliencehub:DescribeAppVersionResourcesResolutionStatus",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeDraftAppVersionResourcesImportStatus",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListAlarmRecommendations",
        "resiliencehub:ListAppAssessmentComplianceDrifts",
        "resiliencehub:ListAppAssessments",
        "resiliencehub:ListAppComponentCompliances",
        "resiliencehub:ListAppComponentRecommendations",
        "resiliencehub:ListAppInputSources",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionAppComponents",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListAppVersionResources",
        "resiliencehub:ListAppVersions",
        "resiliencehub:ListRecommendationTemplates",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListSopRecommendations",
        "resiliencehub:ListSuggestedResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resiliencehub:ListTestRecommendations",
        "resiliencehub:ListUnsupportedAppVersionResources",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
```

```
        "resource-explorer-2:Search",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*",
        "robomaker:List*",
        "route53-recovery-cluster:Get*",
        "route53-recovery-cluster:ListRoutingControls",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:Get*",
        "route53-recovery-readiness:List*",
        "route53:Get*",
        "route53:List*",
        "route53:Test*",
        "route53domains:Check*",
        "route53domains:Get*",
        "route53domains:List*",
        "route53domains:View*",
        "route53resolver:Get*",
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "s3-object-lambda:GetObject",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectLegalHold",
        "s3-object-lambda:GetObjectRetention",
        "s3-object-lambda:GetObjectTagging",
        "s3-object-lambda:GetObjectVersion",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3-object-lambda:GetObjectVersionTagging",
        "s3-object-lambda:ListBucket",
        "s3-object-lambda:ListBucketMultipartUploads",
        "s3-object-lambda:ListBucketVersions",
        "s3-object-lambda:ListMultipartUploadParts",
        "s3:DescribeJob",
        "s3:Get*",
        "s3:List*",
        "sagemaker-groundtruth-synthetic:GetAccountDetails",
        "sagemaker-groundtruth-synthetic:GetBatch",
```

```
        "sagemaker-groundtruth-synthetic:GetProject",
        "sagemaker-groundtruth-synthetic:ListBatchDataTransfers",
        "sagemaker-groundtruth-synthetic:ListBatchSummaries",
        "sagemaker-groundtruth-synthetic:ListProjectDataTransfers",
        "sagemaker-groundtruth-synthetic:ListProjectSummaries",
        "sagemaker:Describe*",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:List*",
        "sagemaker:Search",
        "savingsplans:DescribeSavingsPlanRates",
        "savingsplans:DescribeSavingsPlans",
        "savingsplans:DescribeSavingsPlansOfferingRates",
        "savingsplans:DescribeSavingsPlansOfferings",
        "savingsplans:ListTagsForResource",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:Describe*",
        "schemas:Get*",
        "schemas:List*",
        "schemas:Search*",
        "sdb:Get*",
        "sdb:List*",
        "sdb:Select*",
        "secretsmanager:Describe*",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:List*",
        "securityhub:BatchGetControlEvaluations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "serverlessrepo:Get*",
        "serverlessrepo:List*",
        "serverlessrepo:SearchApplications",
        "servicecatalog:Describe*",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:List*",
        "servicecatalog:Scan*",
        "servicecatalog:Search*",
```

```
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "ses:BatchGetMetricData",
        "ses:Describe*",
        "ses:Get*",
        "ses:List*",
        "shield:Describe*",
        "shield:Get*",
        "shield:List*",
        "signer:DescribeSigningJob",
        "signer:GetSigningPlatform",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningJobs",
        "signer:ListSigningPlatforms",
        "signer:ListSigningProfiles",
        "signer:ListTagsForResource",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeAccountLimits",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeSenderIds",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "snowball:Describe*",
        "snowball:Get*",
```

```
        "snowball:List*",
        "sns:Check*",
        "sns:Get*",
        "sns:List*",
        "sqs:Get*",
        "sqs:List*",
        "sqs:Receive*",
        "ssm-contacts:DescribeEngagement",
        "ssm-contacts:DescribePage",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListEngagements",
        "ssm-contacts:ListPageReceipts",
        "ssm-contacts:ListPagesByContact",
        "ssm-contacts:ListPagesByEngagement",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResourcePolicies",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:ListRelatedItems",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-incidents:ListTimelineEvents",
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Search*",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso:Search*",
        "states:Describe*",
        "states:GetExecutionHistory",
        "states:List*",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "sts:GetAccessKeyInfo",
```

```
        "sts:GetCallerIdentity",
        "sts:GetSessionToken",
        "support:DescribeAttachment",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeTrustedAdvisorCheckRefreshStatuses",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "sustainability:GetCarbonFootprintSummary",
        "swf:Count*",
        "swf:Describe*",
        "swf:Get*",
        "swf:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "tag:DescribeReportCreation",
        "tag:Get*",
        "tax:GetExemptions",
        "tax:GetTaxInheritance",
        "tax:GetTaxInterview",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "timestream:DescribeBatchLoadTask",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListBatchLoadTasks",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "tnb:GetSolFunctionInstance",
        "tnb:GetSolFunctionPackage",
        "tnb:GetSolFunctionPackageContent",
        "tnb:GetSolFunctionPackageDescriptor",
        "tnb:GetSolNetworkInstance",
        "tnb:GetSolNetworkOperation",
```

```
        "tnb:GetSolNetworkPackage",
        "tnb:GetSolNetworkPackageContent",
        "tnb:GetSolNetworkPackageDescriptor",
        "tnb:ListSolFunctionInstances",
        "tnb:ListSolFunctionPackages",
        "tnb:ListSolNetworkInstances",
        "tnb:ListSolNetworkOperations",
        "tnb:ListSolNetworkPackages",
        "tnb:ListTagsForResource",
        "transcribe:Get*",
        "transcribe:List*",
        "transfer:Describe*",
        "transfer:List*",
        "transfer:TestIdentityProvider",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
        "translate:GetTerminology",
        "translate:ListParallelData",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "trustedadvisor:Describe*",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:IsAuthorized",
        "verifiedpermissions:IsAuthorizedWithToken",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListListeners",
```

```
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:Get*",
        "waf-regional:List*",
        "waf:Get*",
        "waf:List*",
        "wafv2:CheckCapacity",
        "wafv2:Describe*",
        "wafv2:Get*",
        "wafv2:List*",
        "wellarchitected:ExportLens",
        "wellarchitected:GetAnswer",
        "wellarchitected:GetConsolidatedReport",
        "wellarchitected:GetLens",
        "wellarchitected:GetLensReview",
        "wellarchitected:GetLensReviewReport",
        "wellarchitected:GetLensVersionDifference",
        "wellarchitected:GetMilestone",
        "wellarchitected:GetProfile",
        "wellarchitected:GetProfileTemplate",
        "wellarchitected:GetReviewTemplate",
        "wellarchitected:GetReviewTemplateAnswer",
        "wellarchitected:GetReviewTemplateLensReview",
        "wellarchitected:GetWorkload",
        "wellarchitected:ListAnswers",
        "wellarchitected:ListCheckDetails",
        "wellarchitected:ListCheckSummaries",
        "wellarchitected:ListLenses",
        "wellarchitected:ListLensReviewImprovements",
        "wellarchitected:ListLensReviews",
        "wellarchitected:ListLensShares",
        "wellarchitected:ListMilestones",
        "wellarchitected:ListNotifications",
        "wellarchitected:ListProfileNotifications",
        "wellarchitected:ListProfiles",
        "wellarchitected:ListProfileShares",
        "wellarchitected:ListReviewTemplateAnswers",
        "wellarchitected:ListReviewTemplates",
```

```
        "wellarchitected:ListShareInvitations",
        "wellarchitected:ListTagsForResource",
        "wellarchitected:ListTemplateShares",
        "wellarchitected:ListWorkloads",
        "wellarchitected:ListWorkloadShares",
        "workdocs:CheckAlias",
        "workdocs:Describe*",
        "workdocs:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:Describe*",
        "xray:BatchGet*",
        "xray:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ResourceGroupsandTagEditorFullAccess

`ResourceGroupsandTagEditorFullAccess`adalah sebuahAWSkebijakan terkelolaitu: Menyediakan akses penuh ke Grup Sumber Daya dan Editor Tag.

Menggunakan kebijakan ini

Anda dapat melampirkan`ResourceGroupsandTagEditorFullAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Tipe:AWSkebijakan terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu yang diedit:10 Agustus 2023, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess`

Versi kebijakan

Versi kebijakan: v6(default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber dayaAWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:getResources",
```

```
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources",
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai denganAWSkebijakan terkelola dan beralih ke izin hak istimewa paling sedikit

ResourceGroupsandTagEditorReadOnlyAccess

`ResourceGroupsandTagEditorReadOnlyAccess`adalah sebuahAWSkebijakan terkelolaitu: Menyediakan akses untuk menggunakan Grup Sumber Daya dan Editor Tag, tetapi tidak mengizinkan pengeditan tag melalui Editor Tag.

Menggunakan kebijakan ini

Anda dapat melampirkan`ResourceGroupsandTagEditorReadOnlyAccess`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Tipe:AWSkebijakan terkelola
- Waktu pembuatan: 06 Februari 2015, 18:39 UTC
- Waktu yang diedit:10 Agustus 2023, 13:42 UTC

- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v3(default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber dayaAWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai denganAWSkebijakan terkelola dan beralih ke izin hak istimewa paling sedikit

ResourceGroupsServiceRolePolicy

`ResourceGroupsServiceRolePolicy`adalah kebijakanAWS terkelola yang: MemungkinkanAWS Resource Groups untuk menanyakanAWS layanan yang memiliki sumber daya Anda untuk menjaga grup up-to-date

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 05 Januari 2023, 16:57 UTC
- Waktu yang telah diedit: 05 Januari 2023, 16.57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
```

```
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ROSAAmazonEBSCSIDriverOperatorPolicy

`ROSAAmazonEBSCSIDriverOperatorPolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Operator DriverOpenShift Amazon EBS Container Storage Interface (CSI) untuk menginstal dan memelihara driver Amazon EBS CSI pada klaster Red HatOpenShift Service onAWS (ROSA). Driver CSI Amazon EBS memungkinkan klaster ROSA mengelola siklus hidup volume Amazon EBS untuk volume persisten.

Menggunakan Kebijakan ini

Anda dapat melampirkan`ROSAAmazonEBSCSIDriverOperatorPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 April 2023, 22:36 UTC
- Waktu yang telah diedit: 20 April 2023, 22.36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotRequestTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

ROSACloudNetworkConfigOperatorPolicy

`ROSACloudNetworkConfigOperatorPolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Operator Pengontrol Config JaringanOpenShift Cloud untuk menyediakan dan mengelola sumber daya jaringan untuk digunakan oleh hamparan jaringan klaster Red HatOpenShift Service onAWS (ROSA). Operator JaringanOpenShift Cloud berinteraksi denganAWS API atas nama plugin jaringan melaluiCustomResourceDefinitions. Operator menggunakan izin kebijakan ini untuk mengelola alamat IP pribadi untuk instans Amazon EC2 sebagai bagian dari klaster ROSA.

Menggunakan kebijakan ini

Anda dapat melampirkan`ROSACloudNetworkConfigOperatorPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 April 2023, 22:34 UTC
- Waktu yang telah diedit: 20 April 2023, 22.34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan yang ditentukan izin untuk kebijakan yang ditentukan. Ketika pengguna atau peran dengan kebijakan membuat permintaan

untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModifyEIPs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center

- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas IAM yang menentukan izin identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ROSAControlPlaneOperatorPolicy

`ROSAControlPlaneOperatorPolicy`adalah kebijakan AWS terkelola yang: Memungkinkan bidang kontrol Red Hat OpenShift Service on AWS (ROSA) untuk mengelola klaster ROSA Amazon EC2 dan sumber daya Amazon Route 53.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAControlPlaneOperatorPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 24 April 2023, 23:02 UTC
- Waktu yang telah diedit: 30 Juni 2023, 21.12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "route53:ListHostedZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "ListResourceRecordSets",
      "Effect" : "Allow",
      "Action" : [
        "route53:ListResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ChangeResourceRecordSetsRestrictedRecordNames",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
```

```
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.hypershift.local"
          ]
        }
      }
    },
    {
      "Sid" : "VPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointResourceTagCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "ManageVPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVPCEndpoingNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
```

```
            "CreateVpcEndpoint",
            "CreateSecurityGroup"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

ROSAImageRegistryOperatorPolicy

`ROSAImageRegistryOperatorPolicy`adalah kebijakan AWS terkelola yang: Memungkinkan Operator Registri OpenShift Gambar menyediakan dan mengelola bucket dan objek Amazon S3 untuk digunakan oleh registri gambar dalam klaster Red Hat OpenShift Service on AWS (ROSA) untuk memenuhi persyaratan penyimpanan ROSA. OpenShift Image Registry Operator menginstal dan memelihara registri internal OpenShift cluster Red Hat.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAImageRegistryOperatorPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 27 April 2023, 20:13 UTC
- Waktu yang telah diedit: 12 Desember 2023, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSpecificBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}"
      ]
    },
```

```
    {
      "Sid" : "AllowSpecificObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*/*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ROSAIngressOperatorPolicy

`ROSAIngressOperatorPolicy`adalah kebijakanAWS terkelola yang: Memungkinkan OperatorOpenShift Ingress untuk menyediakan dan mengelola penyeimbang muatan dan konfigurasi sistem nama domain (DNS) untuk kluster Red HatOpenShift Service onAWS (ROSA). Kebijakan ini memungkinkan akses baca ke nilai tag, yang filter operator untuk sumber daya Route 53 untuk menemukan zona yang dihosting.

Menggunakan kebijakan ini

Anda dapat melampirkan`ROSAIngressOperatorPolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 April 2023, 22:37 UTC
- Waktu yang telah diedit: 20 April 2023, 22.37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "route53:ListHostedZones",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.openshiftapps.com",
            "*.devshift.org",
```

```
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas identitas identitas identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

ROSAInstallerPolicy

`ROSAInstallerPolicy`adalah kebijakan AWS terkelola yang: Memungkinkan penginstal Red Hat OpenShift Service on AWS (ROSA) mengelola AWS sumber daya yang mendukung instalasi cluster ROSA. Ini termasuk mengelola profil instance untuk node pekerja ROSA.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAInstallerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 06 Juni 2023, 21:00 UTC
- Waktu telah diedit: 26 Januari 2024, 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceTypeOfferings",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetOpenIDConnectProvider",
        "iam:GetRole",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53:GetAccountLimit",
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToEC2",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ]
    },
    {
      "Sid" : "CreateInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:TagInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "GetSecretValue",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "Route53ManageRecords",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.hypershift.local",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    },
    {
      "Sid" : "Route53Manage",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeTagsForResource",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTags",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "RunInstancesNoCondition",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RunInstancesRestrictedRequestTag",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesRedHatOwnedAMIs",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822",
            "210686502322"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstancesRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateGrantRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
```

```
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "ManagedKMSRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ROSAKMSProviderPolicy

`ROSAKMSProviderPolicy`adalah kebijakanAWS terkelola yang: Memungkinkan PenyediaAWS Enkripsi ROSA bawaan untuk mengelolaAWS kunci Layanan Manajemen Kunci (KMS) untuk mendukung enkripsi data etcd menggunakan kunciAWS KMS yang disediakan pelanggan. Kebijakan ini memungkinkan enkripsi dan dekripsi data menggunakan kunci KMS.

Menggunakan kebijakan ini

Anda dapat melampirkan`ROSAKMSProviderPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 27 April 2023, 20:10 UTC
- Waktu yang telah diedit: 27 April 2023, 20.10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas identitas
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ROSAKubeControllerPolicy

`ROSAKubeControllerPolicy`adalah kebijakan AWS terkelola yang: Memungkinkan pengontrol ROSA Kubernetes mengelola sumber daya Amazon EC2, Elastic Load Balancing (ELB), AWS dan Key Management Service (KMS) untuk klaster ROSA.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSAKubeControllerPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 27 April 2023, 20:09 UTC
- Waktu yang telah diedit: 16 Oktober 2023, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy`

Versi kebijakan

Versi kebijakan: v3 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
```

```
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeLoadBalancerPolicies"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "LoadBalanacerManagement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancerPolicy",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "CreateTargetGroup",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "LoadBalanacerManagementResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:DeleteLoadBalancerListeners",
        "elasticloadbalancing:AttachLoadBalancerToSubnets",
        "elasticloadbalancing:DetachLoadBalancerFromSubnets",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateListeners",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateListener"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true",
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateLoadBalancer",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ModifySecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ROSAManageSubscription

`ROSAManageSubscription`adalahAWSkebijakan terkelolabahwa: Kebijakan ini menyediakan izin yang diperlukan untuk mengelola Red HatOpenShiftLayanan padaAWS(ROSA) berlangganan.

Menggunakan kebijakan ini

Anda dapat melampirkan`ROSAManageSubscription`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis:AWSkebijakan terkelola
- Waktu pembuatan: 11 April 2022, 20:58 UTC
- Waktu yang diedit:04 Agustus 2023, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/ROSAManageSubscription`

Versi kebijakan

Versi kebijakan: v2(default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber daya,AWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "34850061-abaf-402d-92df-94325c9e947f",
            "bfdca560-2c78-4e64-8193-794c159e6d30"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- MemulaiAWSkebijakan yang dikelola dan beralih ke izin paling tidak memiliki hak istimewa

ROSANodePoolManagementPolicy

`ROSANodePoolManagementPolicy`adalah kebijakan AWS terkelola yang: Memungkinkan Red Hat OpenShift Service on AWS (ROSA) mengelola instans EC2 klaster sebagai node pekerja, termasuk izin untuk mengonfigurasi grup keamanan dan instance tag dan volume. Kebijakan ini juga memungkinkan penggunaan instans EC2 dengan enkripsi disk yang disediakan oleh AWS kunci Key Management Service (KMS).

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSANodePoolManagementPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 08 Juni 2023, 20:48 UTC
- Waktu yang telah diedit: 08 Juni 2023, 20.48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy`

Versi kebijakan

Versi kebijakan: v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassWorkerRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AuthorizeSecurityGroupIngressRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfacesNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesRequest",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "RunInstancesRedHatAMI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822"
          ]
        }
      }
    },
    {
      "Sid" : "ManagedKMSRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateGrantRestricted",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling sedikit hak istimewa

ROSASRESupportPolicy

`ROSASRESupportPolicy`adalah kebijakan AWS terkelola yang: Menyediakan rekayasa keandalan situs ROSA (SRE) izin yang diperlukan untuk awalnya mengamati, mendiagnosis, dan mendukung AWS sumber daya yang terkait dengan kluster Red Hat OpenShift Service on AWS (ROSA), termasuk kemampuan untuk mengubah status node cluster ROSA.

Menggunakan kebijakan ini

Anda dapat melampirkan `ROSASRESupportPolicy` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 01 Juni 2023, 14:36 UTC
- Waktu telah diedit: 22 Januari 2024, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "sts:DecodeAuthorizationMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHostedZoneCount",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DecribeIAMRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2DescribeInstance",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeScheduledInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "VPCNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Cloudtrail",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Cloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "DescribeVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeLoadBalancers",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpoints"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeAddressesAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeAddressesAttribute",
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*"
    },
    {
      "Sid" : "DescribeInstance",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeSpotFleetInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSpotFleetInstances",
      "Resource" : "arn:aws:ec2:*:*:spot-fleet-request/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "DescribeVolumeAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeVolumeAttribute",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ManageInstanceLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ROSAWorkerInstancePolicy

`ROSAWorkerInstancePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan node pekerja Red HatOpenShift Service onAWS (ROSA) di akses hanya-baca akun Anda ke instans Amazon EC2 danWilayah AWS untuk manajemen siklus hidup node komputasi.

Menggunakan kebijakan ini

Anda dapat melampirkan`ROSAWorkerInstancePolicy` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 April 2023, 22:35 UTC
- Waktu yang telah diedit: 20 April 2023, 22.35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan Jasa Jasa Jet untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

Route53RecoveryReadinessServiceRolePolicy

`Route53RecoveryReadinessServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan Peran Tertaut Layanan untuk Kesiapan Pemulihan Route 53

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, atau peran tidak dapat dilampirkan pada pengguna, atau peran tidak dapat dilampirkan pada pengguna, atau

detail kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 15 Juli 2021, 16:06 UTC
- Waktu yang telah diedit: 14 Februari 2023, 18.08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v5 (default)

Versi default default adalah versi yang menentukan izin untuk kebijakan default. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicequotas.amazonaws.com/
AWSServiceRoleForServiceQuotas",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:ListAliases",
        "lambda:ListVersionsByFunction"
```

```
      ],
      "Resource" : "arn:aws:lambda:*:*:function:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBClusters"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ListResourceRecordSets"
      ],
      "Resource" : "arn:aws:route53:::hostedzone/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHealthCheck",
        "route53:GetHealthCheckStatus"
      ],
      "Resource" : "arn:aws:route53:::healthcheck/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:RequestServiceQuotaIncrease"
      ],
      "Resource" : "arn:aws:servicequotas:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic"
```

```
      ],
      "Resource" : "arn:aws:sns:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ],
      "Resource" : "arn:aws:sqs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeLoadBalancerTargetGroups",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribePolicies",
        "cloudwatch:GetMetricData",
        "cloudwatch:DescribeAlarms",
        "dynamodb:DescribeLimits",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
```

```
        "elasticloadbalancing:DescribeTargetHealth",
        "kafka:DescribeCluster",
        "kafka:DescribeConfigurationRevision",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "rds:DescribeAccountAttributes",
        "route53:GetHostedZone",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "sns:GetEndpointAttributes",
        "sns:GetSubscriptionAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

Route53ResolverServiceRolePolicy

`Route53ResolverServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan akses keLayanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Route53 Resolver

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 12 Agustus 2020, 17:47 UTC

- Waktu yang telah diedit: 12 Agustus 2020 17.47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan ini adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan SON SON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "s3:GetBucketPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

S3StorageLensServiceRolePolicy

`S3StorageLensServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan akses keLayanan AWS dan Sumber Daya yang digunakan atau dikelola oleh S3 Storage Lens

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini pada pengguna, grup grup, grup grup, grup, grup, grup, grup, grup, grup, grup, grup

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 18 November 2020, 18:15 UTC
- Waktu yang telah diedit: 18 November 2020, 18.15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan kebijakan kebijakan kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
```

```
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

SecretsManagerReadWrite

`SecretsManagerReadWrite`adalah kebijakan AWS terkelola yang: Menyediakan akses baca/tulis ke AWS Secrets Manager melalui. AWS Management Console Catatan: ini mengeluarkan tindakan IAM, jadi gabungkan dengan IAM FullAccess jika konfigurasi rotasi diperlukan.

Menggunakan kebijakan ini

Anda dapat melampirkan `SecretsManagerReadWrite` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 04 April 2018, 18:05 UTC
- Waktu telah diedit: 22 Februari 2024, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/SecretsManagerReadWrite`

Versi kebijakan

Versi kebijakan: v5 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:*",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys",
        "lambda:ListFunctions",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
```

```
      "Resource" : "arn:aws:lambda:*:*:function:SecretsManager*"
    },
    {
      "Sid" : "SARPermissions",
      "Effect" : "Allow",
      "Action" : [
        "serverlessrepo:CreateCloudFormationChangeSet",
        "serverlessrepo:GetApplication"
      ],
      "Resource" : "arn:aws:serverlessrepo:*:*:applications/SecretsManager*"
    },
    {
      "Sid" : "S3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::awsserverlessrepo-changesets*",
        "arn:aws:s3:::secrets-manager-rotation-apps-*/*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SecurityAudit

`SecurityAudit`adalah kebijakan AWS terkelola yang: Templat audit keamanan memberikan akses untuk membaca metadata konfigurasi keamanan. Ini berguna untuk perangkat lunak yang mengaudit konfigurasi file. Akun AWS

Menggunakan kebijakan ini

Anda dapat melampirkan `SecurityAudit` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 14 Desember 2023, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/SecurityAudit`

Versi kebijakan

Versi kebijakan: v41 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "BaseSecurityAuditStatement",
      "Action" : [
        "a4b:ListSkills",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
```

```
        "account:GetRegionOptStatus",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetPolicy",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags",
        "acm:Describe*",
        "acm:List*",
        "airflow:ListEnvironments",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appsync:GetApiCache",
        "appsync:List*",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:ListAssessmentControlInsightsByControlDomain",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentFrameworkShareRequests",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListAssessments",
        "auditmanager:ListControlDomainInsights",
        "auditmanager:ListControlDomainInsightsByAssessment",
        "auditmanager:ListControlInsightsByControlDomain",
        "auditmanager:ListControls",
        "auditmanager:ListNotifications",
```

```
        "auditmanager:ListTagsForResource",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling:Describe*",
        "backup:DescribeRegionSettings",
        "backup:GetBackupVaultAccessPolicy",
        "backup:ListBackupVaults",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobDefinitions",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "chime:List*",
        "cloud9:Describe*",
        "cloud9:ListEnvironments",
        "clouddirectory:ListDirectories",
        "cloudformation:DescribeStack*",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListStack*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:DescribeDomainEndpointOptions",
        "cloudsearch:DescribeDomains",
        "cloudsearch:DescribeServiceAccessPolicies",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListTags",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GetDashboard",
        "cloudwatch:ListTagsForResource",
        "cloudwatch:ListDashboards",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListRepositories",
        "codebuild:BatchGetProjects",
        "codebuild:ListProjects",
        "codecommit:BatchGetRepositories",
        "codecommit:GetBranch",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:List*",
```

```
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:GetJobDetails",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelines",
        "codestar:Describe*",
        "codestar:List*",
        "cognito-identity:Describe*",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:Describe*",
        "cognito-idp:ListDevices",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserImportJobs",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListUsersInGroup",
        "cognito-sync:Describe*",
        "cognito-sync:List*",
        "comprehend:Describe*",
        "comprehend:List*",
        "comprehendmedical:ListICD10CMInferenceJobs",
        "comprehendmedical:ListPHIDetectionJobs",
        "comprehendmedical:ListRxNormInferenceJobs",
        "comprehendmedical:ListSNOMEDCTInferenceJobs",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "connect:ListInstances",
        "dataexchange:ListDataSets",
        "datapipeline:DescribeObjects",
```

```
        "datapipeline:DescribePipelines",
        "datapipeline:EvaluateExpression",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "datapipeline:ValidatePipelineDefinition",
        "datasync:Describe*",
        "datasync:List*",
        "dax:Describe*",
        "dax:ListTags",
        "deepracer:ListModels",
        "detective:GetGraphIngestState",
        "detective:ListGraphs",
        "detective:ListMembers",
        "devicefarm:ListProjects",
        "directconnect:Describe*",
        "discovery:DescribeAgents",
        "discovery:DescribeConfigurations",
        "discovery:DescribeContinuousExports",
        "discovery:DescribeExportConfigurations",
        "discovery:DescribeExportTasks",
        "discovery:DescribeImportTasks",
        "dms:Describe*",
        "dms:ListTagsForResource",
        "docdb-elastic:ListClusters",
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListBackups",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
```

```
        "ec2:GetTransitGatewayPrefixListReferences",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribeImages",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodeGroup",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodeGroups",
        "eks:ListUpdates",
        "elastic-inference:DescribeAccelerators",
        "elasticache:Describe*",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:ListTagsForResource",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
```

```
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elastictranscoder:ListPipelines",
        "es:Describe*",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListElasticsearchInstanceTypeDetails",
        "es:ListElasticsearchVersions",
        "es:ListTags",
        "events:Describe*",
        "events:List*",
        "events:TestEventPattern",
        "finspace:ListEnvironments",
        "finspace:ListKxEnvironments",
        "firehose:Describe*",
        "firehose:List*",
        "fms:ListComplianceStatus",
        "fms:ListPolicies",
        "forecast:ListDatasets",
        "frauddetector:GetDetectors",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "geo:ListMaps",
        "glacier:DescribeVault",
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultLock",
        "glacier:ListVaults",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:GetCrawlers",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDevEndpoints",
        "glue:GetJobs",
        "glue:GetResourcePolicy",
        "glue:GetSecurityConfigurations",
```

```
        "grafana:ListWorkspaces",
        "greengrass:List*",
        "guardduty:DescribePublishingDestination",
        "guardduty:Get*",
        "guardduty:List*",
        "health:DescribeAffectedEntities",
        "health:DescribeEntityAggregates",
        "health:DescribeEventAggregates",
        "health:DescribeEvents",
        "health:DescribeEventTypes",
        "healthlake:ListFHIRDatastores",
        "honeycode:ListTables",
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "iot:Describe*",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:List*",
        "iotanalytics:ListChannels",
        "iotevents:ListInputs",
```

```
        "iotfleetwise:ListModelManifests",
        "iotsitewise:DescribeGatewayCapabilityConfiguration",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListGateways",
        "iottwinmaker:ListWorkspaces",
        "kafka-cluster:Describe*",
        "kafka:Describe*",
        "kafka:GetBootstrapBrokers",
        "kafka:GetCompatibleKafkaVersions",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kinesis:DescribeLimits",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListShards",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:ListApplications",
        "kinesisvideo:DescribeEdgeConfiguration",
        "kinesisvideo:DescribeMappedResourceConfiguration",
        "kinesisvideo:DescribeMediaStorageConfiguration",
        "kinesisvideo:DescribeNotificationConfiguration",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lambda:GetAccountSettings",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:List*",
        "lex:DescribeBot",
        "lex:DescribeResourcePolicy",
```

```
        "lex:ListBots",
        "license-manager:List*",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancers",
        "logs:Describe*",
        "logs:ListTagsLogGroup",
        "lookoutequipment:ListDatasets",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutvision:ListProjects",
        "machinelearning:DescribeMLModels",
        "managedblockchain:ListNetworks",
        "mechanicalturk:ListHITs",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:ListChannels",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:DescribeOriginEndpoint",
        "mediapackage:ListOriginEndpoints",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:ListContainers",
        "memorydb:DescribeClusters",
        "mq:DescribeBroker",
        "mq:DescribeBrokerEngineTypes",
        "mq:DescribeBrokerInstanceOptions",
        "mq:DescribeConfiguration",
        "mq:DescribeConfigurationRevision",
        "mq:DescribeUser",
        "mq:ListBrokers",
        "mq:ListConfigurationRevisions",
        "mq:ListConfigurations",
        "mq:ListTags",
        "mq:ListUsers",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
```

```
        "networkmanager:DescribeGlobalNetworks",
        "nimble:ListStudios",
        "opsworks-cm:DescribeServers",
        "opsworks:DescribeStacks",
        "organizations:Describe*",
        "organizations:List*",
        "personalize:DescribeDatasetGroup",
        "personalize:ListDatasetGroups",
        "private-networks:ListNetworks",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "quicksight:Describe*",
        "quicksight:List*",
        "ram:GetResourceShares",
        "ram:List*",
        "rds:Describe*",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource",
        "redshift:Describe*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resource-groups:ListGroupResources",
        "robomaker:Describe*",
        "robomaker:List*",
        "route53:Get*",
        "route53:List*",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:ListDomains",
        "route53domains:ListOperations",
        "route53domains:ListTagsForDomain",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListOutpostsWithS3",
        "s3-outposts:ListSharedEndpoints",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessPoint",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccountPublicAccessBlock",
```

```
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucket*",
        "s3:GetEncryptionConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:GetReplicationConfiguration",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "sdb:DomainMetadata",
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "serverlessrepo:GetApplicationPolicy",
        "serverlessrepo:List*",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListServiceQuotas",
```

```
        "servicequotas:ListServices",
        "servicequotas:ListTagsForResource",
        "ses:Describe*",
        "ses:GetAccountSendingEnabled",
        "ses:GetIdentityDkimAttributes",
        "ses:GetIdentityPolicies",
        "ses:GetIdentityVerificationAttributes",
        "ses:ListConfigurationSets",
        "ses:ListIdentities",
        "ses:ListIdentityPolicies",
        "ses:ListReceiptRuleSets",
        "ses:ListVerifiedEmailAddresses",
        "shield:Describe*",
        "shield:GetSubscriptionState",
        "shield:List*",
        "snowball:ListClusters",
        "snowball:ListJobs",
        "sns:GetPlatformApplicationAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:Describe*",
        "ssm:GetAutomationExecution",
        "ssm:ListAssociations",
        "ssm:ListAssociationVersions",
        "ssm:ListCommands",
        "ssm:ListComplianceItems",
        "ssm:ListComplianceSummaries",
        "ssm:ListDocumentMetadataHistory",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "ssm:ListInventoryEntries",
        "ssm:ListOpsMetadata",
        "ssm:ListResourceComplianceSummaries",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso:DescribeAccountAssignmentCreationStatus",
        "sso:DescribePermissionSet",
```

```
        "sso:DescribePermissionsPolicies",
        "sso:List*",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "storagegateway:DescribeBandwidthRateLimit",
        "storagegateway:DescribeCache",
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:DescribeMaintenanceStartTime",
        "storagegateway:DescribeNFSFileShares",
        "storagegateway:DescribeSnapshotSchedule",
        "storagegateway:DescribeStorediSCSIVolumes",
        "storagegateway:DescribeTapeArchives",
        "storagegateway:DescribeTapeRecoveryPoints",
        "storagegateway:DescribeTapes",
        "storagegateway:DescribeUploadBuffer",
        "storagegateway:DescribeVTLDevices",
        "storagegateway:DescribeWorkingStorage",
        "storagegateway:List*",
        "sts:GetAccessKeyInfo",
        "support:DescribeTrustedAdvisorCheckRefreshStatuses",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "tag:GetTagKeys",
        "transcribe:GetCallAnalyticsCategory",
        "transcribe:GetMedicalVocabulary",
        "transcribe:GetVocabulary",
        "transcribe:GetVocabularyFilter",
        "transcribe:ListCallAnalyticsCategories",
        "transcribe:ListCallAnalyticsJobs",
        "transcribe:ListLanguageModels",
        "transcribe:ListMedicalTranscriptionJobs",
```

```
        "transcribe:ListMedicalVocabularies",
        "transcribe:ListTagsForResource",
        "transcribe:ListTranscriptionJobs",
        "transcribe:ListVocabularies",
        "transcribe:ListVocabularyFilters",
        "transfer:Describe*",
        "transfer:List*",
        "translate:List*",
        "trustedadvisor:Describe*",
        "waf-regional:GetWebACL",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:ListTagsForResource",
        "waf-regional:ListWebACLs",
        "waf:GetWebACL",
        "waf:ListTagsForResource",
        "waf:ListWebACLs",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLforResource",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:ListIPSets",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListResourcesForWebACL",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "wafv2:ListWebACLs",
        "workdocs:DescribeResourcePermissions",
        "workspaces:Describe*",
        "xray:GetEncryptionConfig",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetTraceSummaries",
        "xray:ListTagsForResource"
      ]
    },
    {
      "Effect" : "Allow",
      "Sid" : "APIGatewayAccess",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
```

```
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/cors",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/exports/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
```

```
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

SecurityLakeServiceLinkedRole

`SecurityLakeServiceLinkedRole`adalah kebijakan AWS terkelola yang: Kebijakan ini memberikan izin untuk mengoperasikan layanan Amazon Security Lake atas nama Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran terkait layanan
- Waktu pembuatan: 29 November 2022, 14:03 UTC
- Waktu telah diedit: 29 Februari 2024, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Saat pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan tersebut.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsPolicies",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeOrgAccounts",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/o-*/*"
      ]
    },
    {
      "Sid" : "AllowManagementOfServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel",
        "cloudtrail:GetServiceLinkedChannel",
        "cloudtrail:UpdateServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-lake/*"
    },
    {
      "Sid" : "AllowListServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListServiceLinkedChannels"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeAnyVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListDelegatedAdmins",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowWafLoggingConfiguration",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListLoggingConfigurations",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "wafv2:LogScope" : "SecurityLake"
        }
      }
    },
    {
      "Sid" : "AllowPutLoggingConfiguration",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "wafv2:LogDestinationResource" : "arn:aws:s3:::aws-waf-logs-security-lake-*"
        }
      }
    },
    {
      "Sid" : "ListWebACLs",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:ListWebACLs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami pembuatan versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit

ServerMigration_ServiceRole

`ServerMigration_ServiceRole`adalah kebijakanAWS terkelola yang: Izin untuk memungkinkan Layanan MigrasiAWS Server untuk memigrasi VM ke EC2: memungkinkan Layanan Migrasi Server untuk menempatkan sumber daya yang dimigrasi ke akun EC2 pelanggan.

Menggunakan kebijakan ini

Anda dapat melampirkan`ServerMigration_ServiceRole` ke pengguna, grup, dan peran Anda.

Detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 11 Agustus 2020, 20:41 UTC
- Waktu yang telah diedit: 15 Oktober 2020, 17.26 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*",
      "Condition" : {
        "Null" : {
          "cloudformation:ResourceTypes" : "false"
        },
        "ForAllValues:StringEquals" : {
          "cloudformation:ResourceTypes" : [
            "AWS::EC2::Instance",
            "AWS::ApplicationInsights::Application",
            "AWS::ResourceGroups::Group"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DescribeChangeSet",
```

```
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::sms-app-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:CreateReplicationJob",
        "sms:DeleteReplicationJob",
        "sms:GetReplicationJobs",
        "sms:GetReplicationRuns",
        "sms:GetServers",
        "sms:ImportServerCatalog",
        "sms:StartOnDemandReplicationRun",
        "sms:UpdateReplicationJob"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunRemoteScript",
        "arn:aws:s3:::sms-app-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/UseForSMSApplicationValidation" : [
            "true"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DeregisterImage",
        "ec2:ImportImage",
        "ec2:DescribeImportImageTasks",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "cloudformation.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

ServerMigrationConnector

`ServerMigrationConnector`adalah kebijakanAWS terkelola yang: Izin untuk memungkinkan Konektor MigrasiAWS Server untuk memigrasi VM ke EC2. Memungkinkan komunikasi dengan Layanan MigrasiAWS Server, akses baca/tulis ke bucket S3 dimulai dengan 'sms-b-' dan 'import-to-ec2-' serta bucket yang digunakan untuk upgrade Konektor MigrasiAWS Server, pendaftaran Konektor MigrasiAWS Server denganAWS, dan metrik mengunggah keAWS.

Menggunakan kebijakan ini

Anda dapat melampirkan`ServerMigrationConnector` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Oktober 2016 21:45 UTC
- Waktu yang telah diedit: 24 Oktober 2016 21.45 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationConnector`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:SendMessage",
        "sms:GetMessages"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutLifecycleConfiguration",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3:::sms-b-*",
        "arn:aws:s3:::import-to-ec2-*",
        "arn:aws:s3:::server-migration-service-upgrade",
        "arn:aws:s3:::server-migration-service-upgrade/*",
        "arn:aws:s3:::connector-platform-upgrade-info/*",
        "arn:aws:s3:::connector-platform-upgrade-info",
        "arn:aws:s3:::connector-platform-upgrade-bundles/*",
        "arn:aws:s3:::connector-platform-upgrade-bundles",
        "arn:aws:s3:::connector-platform-release-notes/*",
        "arn:aws:s3:::connector-platform-release-notes"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "awsconnector:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ServerMigrationServiceConsoleFullAccess

`ServerMigrationServiceConsoleFullAccess`adalah kebijakanAWS terkelola yang: Izin yang diperlukan untuk menggunakan semua fitur Konsol Layanan Migrasi Server

Menggunakan kebijakan ini

Anda dapat melampirkan`ServerMigrationServiceConsoleFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 09 Mei 2020, 17:18 UTC
- Waktu yang telah diedit: 20 Juli 2020, 22.00 UTC

- ARN: `arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sms:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "s3:ListAllMyBuckets",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
```

```
      "Action" : [
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "sms.amazonaws.com"
        }
      },
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ServerMigrationServiceLaunchRole

`ServerMigrationServiceLaunchRole`adalah kebijakanAWS terkelola yang: Izin untuk memungkinkan Layanan MigrasiAWS Server untuk membuat dan memperbaruiAWS sumber daya yang relevan ke pelangganAkun AWS untuk meluncurkan server dan aplikasi yang dimigrasi.

Menggunakan kebijakan ini

Anda dapat melampirkan`ServerMigrationServiceLaunchRole` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 26 November 2018, 19:53 UTC
- Waktu yang telah diedit: 15 Oktober 2020 17.29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:Describe*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:CreateApplication",
        "applicationinsights:CreateComponent",
        "applicationinsights:UpdateApplication",
        "applicationinsights:DeleteApplication",
        "applicationinsights:UpdateComponentConfiguration",
        "applicationinsights:DeleteComponent"
      ],
      "Resource" : "arn:aws:applicationinsights:*:*:application/resource-group/sms-app-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:GetGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/sms-app-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ServerMigrationServiceRoleForInstanceValidation

`ServerMigrationServiceRoleForInstanceValidation`adalah kebijakanAWS terkelola yang: Izin untuk memungkinkanAWS SMS menjalankan skrip validasi data bekas dan mengirim kesuksesan skrip/kegagalan kembali ke SMS

Menggunakan kebijakan ini

Anda dapat melampirkan`ServerMigrationServiceRoleForInstanceValidation` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 20 Juli 2020, 22:25 UTC

- Waktu yang telah diedit: 20 Juli 2020, 22.25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ServiceQuotasFullAccess

`ServiceQuotasFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Service Quotas

Menggunakan kebijakan ini

Anda dapat melampirkan`ServiceQuotasFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Juni 2019, 15:44 UTC
- Waktu yang telah diedit: 04 Februari 2021 09.29 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasFullAccess`

Versi kebijakan

Versi kebijakan:v4 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "dynamodb:DescribeLimits",
```

```
        "elasticloadbalancing:DescribeAccountLimits",
        "iam:GetAccountSummary",
        "kinesis:DescribeLimits",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "rds:DescribeAccountAttributes",
        "route53:GetAccountLimit",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "servicequotas:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/ServiceQuotaMonitor" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "servicequotas.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
      }
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ServiceQuotasReadOnlyAccess

`ServiceQuotasReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses baca saja ke Service Quotas

Menggunakan kebijakan ini

Anda dapat melampirkan`ServiceQuotasReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 24 Juni 2019, 15:31 UTC
- Waktu yang telah diedit: 21 Desember 2020 18.11 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "dynamodb:DescribeLimits",
        "elasticloadbalancing:DescribeAccountLimits",
        "iam:GetAccountSummary",
        "kinesis:DescribeLimits",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "rds:DescribeAccountAttributes",
        "route53:GetAccountLimit",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServices",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListTagsForResource"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

ServiceQuotasServiceRolePolicy

`ServiceQuotasServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan Service Quotas untuk membuat kasus dukungan atas nama Anda

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 22 Mei 2019, 20:44 UTC
- Waktu yang telah diedit: 24 Juni 2019 14.52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

SimpleWorkflowFullAccess

`SimpleWorkflowFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke layanan konfigurasi Alur Kerja Sederhana.

Menggunakan kebijakan ini

Anda dapat melampirkan`SimpleWorkflowFullAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 06 Februari 2015, 18:41 UTC
- Waktu yang telah diedit: 06 Pebruari 2015 18.41 UTC
- ARN: `arn:aws:iam::aws:policy/SimpleWorkflowFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "swf:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

SupportUser

`SupportUser`adalah sebuahAWSkebijakan terkelolabahwa: Kebijakan ini memberikan izin untuk memecahkan masalah dan menyelesaikan masalah diAkun AWS. Kebijakan ini juga memungkinkan pengguna untuk menghubungiAWSdukungan untuk membuat dan mengelola kasus.

Menggunakan kebijakan ini

Anda dapat melampirkan`SupportUser`untuk pengguna, grup, dan peran Anda.

Rincian kebijakan

- Tipe: Kebijakan fungsi pekerjaan
- Waktu pembuatan: 10 November 2016, 17:21 UTC
- Waktu yang diedit:25 Agustus 2023, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SupportUser`

Versi kebijakan

Versi kebijakan: v8(default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWSsumber dayaAWSmemeriksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*",
        "acm:DescribeCertificate",
        "acm:GetCertificate",
        "acm:List*",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities",
        "apigateway:GET",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:Describe*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:EstimateTemplateCost",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
```

```
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents",
        "cloudtrail:ListTags",
        "cloudtrail:ListPublicKeys",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codecommit:BatchGetRepositories",
        "codecommit:Get*",
        "codecommit:List*",
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:AcknowledgeJob",
        "codepipeline:AcknowledgeThirdPartyJob",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:PollForJobs",
        "codepipeline:PollForThirdPartyJobs",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipeline",
        "cognito-identity:List*",
        "cognito-identity:LookupDeveloperIdentity",
        "cognito-identity:Describe*",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeRiskConfiguration",
        "cognito-idp:DescribeUserImportJob",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:List*",
        "cognito-sync:Describe*",
        "cognito-sync:GetBulkPublishDetails",
        "cognito-sync:GetCognitoEvents",
        "cognito-sync:GetIdentityPoolConfiguration",
        "cognito-sync:List*",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetResourceConfigHistory",
        "config:ListDiscoveredResources",
```

```
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "datapipeline:ReportTaskProgress",
        "datapipeline:ReportTaskRunnerHeartbeat",
        "devicefarm:List*",
        "devicefarm:Get*",
        "directconnect:Describe*",
        "discovery:Describe*",
        "discovery:ListConfigurations",
        "dms:Describe*",
        "dms:List*",
        "ds:DescribeDirectories",
        "ds:DescribeSnapshots",
        "ds:GetDirectoryLimits",
        "ds:GetSnapshotLimits",
        "ds:ListAuthorizedApplications",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:Describe*",
        "ec2:DescribeHosts",
        "ec2:describeIdentityIdFormat",
        "ec2:DescribeIdFormat",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeNatGateways",
        "ec2:DescribeReservedInstancesModifications",
        "ec2:DescribeTags",
        "ec2:SearchLocalGatewayRoutes",
        "ecr:GetRepositoryPolicy",
        "ecr:BatchCheckLayerAvailability",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:Describe*",
        "ecs:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
```

```
        "elasticbeanstalk:ValidateConfigurationSettings",
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elastictranscoder:List*",
        "elastictranscoder:ReadJob",
        "elasticfilesystem:DescribeFileSystems",
        "es:Describe*",
        "es:List*",
        "es:ESHttpGet",
        "es:ESHttpHead",
        "events:DescribeRule",
        "events:List*",
        "events:TestEventPattern",
        "firehose:Describe*",
        "firehose:List*",
        "gamelift:List*",
        "gamelift:Describe*",
        "glacier:ListVaults",
        "glacier:DescribeVault",
        "glacier:DescribeJob",
        "glacier:Get*",
        "glacier:List*",
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "importexport:GetStatus",
        "importexport:ListJobs",
        "inspector:Describe*",
        "inspector:List*",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:DiscoverInputSchema",
        "kinesisanalytics:GetApplicationState",
        "kinesisanalytics:ListApplications",
        "kinesis:Describe*",
        "kinesis:Get*",
        "kinesis:List*",
        "kms:Describe*",
        "kms:Get*",
```

```
        "kms:List*",
        "lambda:List*",
        "lambda:Get*",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "machinelearning:Describe*",
        "machinelearning:Get*",
        "opsworks:Describe*",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "redshift:Describe*",
        "route53:Get*",
        "route53:List*",
        "route53domains:CheckDomainAvailability",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:List*",
        "s3:List*",
        "sdb:GetAttributes",
        "sdb:List*",
        "sdb:Select*",
        "servicecatalog:SearchProducts",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ScanProvisionedProducts",
        "ses:Get*",
        "ses:List*",
        "sns:Get*",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListQueues",
        "sqs:ReceiveMessage",
        "ssm:List*",
        "ssm:Describe*",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "swf:Count*",
        "swf:Describe*",
        "swf:Get*",
```

```
        "swf:List*",
        "waf:Get*",
        "waf:List*",
        "workdocs:Describe*",
        "workmail:Describe*",
        "workmail:Get*",
        "workspaces:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Buat set izin menggunakanAWSkebijakan terkelola di Pusat Identitas IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami pembuatan versi untuk kebijakan IAM
- Memulai denganAWSkebijakan terkelola dan beralih ke izin hak istimewa paling sedikit

SystemAdministrator

`SystemAdministrator`adalah kebijakanAWS terkelola yang: Memberikan izin akses penuh yang diperlukan untuk sumber daya yang diperlukan untuk operasi aplikasi dan pengembangan.

Menggunakan kebijakan ini

Anda dapat melampirkan`SystemAdministrator` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan fungsi Job
- Waktu pembuatan: 10 November 2016, 17:23 UTC
- Waktu yang telah diedit: 24 Agustus 2020, 20.05 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SystemAdministrator`

Versi kebijakan

Versi kebijakan:v6 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "acm:Request*",
        "acm:Resend*",
        "autoscaling:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListPublicKeys",
        "cloudtrail:ListTags",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudwatch:*",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateBranch",
        "codecommit:CreateRepository",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:List*",
        "codecommit:Put*",
        "codecommit:Test*",
        "codecommit:Update*",
        "codedeploy:*",
        "codepipeline:*",
        "config:*",
        "ds:*",
        "ec2:Allocate*",
```

```
        "ec2:AssignPrivateIpAddresses*",
        "ec2:Associate*",
        "ec2:Allocate*",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:Bundle*",
        "ec2:Cancel*",
        "ec2:Copy*",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDhcpOptions",
        "ec2:CreateFlowLogs",
        "ec2:CreateImage",
        "ec2:CreateInstanceExportTask",
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreatePlacementGroup",
        "ec2:CreateReservedInstancesListing",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateSpotDatafeedSubscription",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteKeyPair",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInterface",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteSpotDatafeedSubscription",
```

```
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DeregisterImage",
        "ec2:Describe*",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVolumeIO",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetConsoleOutput",
        "ec2:GetHostReservationPurchasePreview",
        "ec2:GetLaunchTemplateData",
        "ec2:GetPasswordData",
        "ec2:Import*",
        "ec2:Modify*",
        "ec2:MonitorInstances",
        "ec2:MoveAddressToVpc",
        "ec2:Purchase*",
        "ec2:RegisterImage",
        "ec2:Release*",
        "ec2:Replace*",
        "ec2:ReportInstanceStatus",
        "ec2:Request*",
        "ec2:Reset*",
        "ec2:RestoreAddressToClassic",
        "ec2:RunScheduledInstances",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UnmonitorInstances",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "elasticloadbalancing:*",
        "events:*",
        "iam:GetAccount*",
        "iam:GetContextKeys*",
```

```
        "iam:GetCredentialReport",
        "iam:ListAccountAliases",
        "iam:ListGroups",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListPoliciesGrantingServiceAccess",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:Simulate*",
        "iam:UpdateServerCertificate",
        "iam:UpdateSigningCertificate",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms:DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
        "kms:List*",
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "lambda:Create*",
        "lambda:Delete*",
        "lambda:Get*",
        "lambda:InvokeFunction",
        "lambda:List*",
        "lambda:PublishVersion",
        "lambda:Update*",
        "logs:*",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "route53:*",
        "route53domains:*",
        "ses:*",
        "sns:*",
        "sqs:*",
        "trustedadvisor:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
```

```
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AttachClassicLinkVpc",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVpcPeeringConnection",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNetworkAcl*",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DetachClassicLinkVpc",
        "ec2:DetachVolume",
        "ec2:DisableVpcClassicLink",
        "ec2:EnableVpcClassicLink",
        "ec2:GetConsoleScreenshot",
        "ec2:RebootInstances",
        "ec2:RejectVpcPeeringConnection",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "s3:*",
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
```

```
        "iam:GetAccessKeyLastUsed",
        "iam:GetGroup*",
        "iam:GetInstanceProfile",
        "iam:GetLoginProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy*",
        "iam:GetRole*",
        "iam:GetSAMLProvider",
        "iam:GetSSHPublicKey",
        "iam:GetServerCertificate",
        "iam:GetServiceLastAccessed*",
        "iam:GetUser*",
        "iam:ListAccessKeys",
        "iam:ListAttached*",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles*",
        "iam:ListMFADevices",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListSSHPublicKeys",
        "iam:ListSigningCertificates",
        "iam:ListUserPolicies",
        "iam:Upload*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/rds-monitoring-role",
        "arn:aws:iam::*:role/ec2-sysadmin-*",
        "arn:aws:iam::*:role/ecr-sysadmin-*",
        "arn:aws:iam::*:role/lambda-sysadmin-*"
      ]
```

```
    }
  ],
  "Version" : "2012-10-17"
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

TranslateFullAccess

`TranslateFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon Translate.

Menggunakan kebijakan ini

Anda dapat melampirkan`TranslateFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 27 November 2018, 23:36 UTC
- Waktu yang telah diedit: 08 Januari 2020, 21.22 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateFullAccess`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "translate:*",
        "comprehend:DetectDominantLanguage",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

TranslateReadOnly

`TranslateReadOnly`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya-baca ke Amazon Translate.

Menggunakan kebijakan ini

Anda dapat melampirkan `TranslateReadOnly` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2017, 18:22 UTC
- Waktu yang telah diedit: 24 Mei 2023, 17.19 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateReadOnly`

Versi kebijakan

Versi kebijakan: v7 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "translate:TranslateText",
        "translate:TranslateDocument",
        "translate:GetTerminology",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
        "translate:ListParallelData",
        "comprehend:DetectDominantLanguage",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling sedikit hak istimewa

ViewOnlyAccess

`ViewOnlyAccess`adalah kebijakanAWS terkelola yang: Kebijakan ini memberikan izin untuk melihat sumber daya dan metadata dasar di semuaAWS layanan.

Menggunakan kebijakan ini

Anda dapat melampirkan`ViewOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan fungsi Job
- Waktu pembuatan: 10 November 2016, 17:20 UTC
- Waktu yang telah diedit: 06 Maret 2023, 15.59 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

Versi kebijakan

Versi kebijakan:v17 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Action" : [
        "acm:ListCertificates",
        "athena:List*",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "batch:ListJobs",
        "clouddirectory:ListAppliedSchemaArns",
        "clouddirectory:ListDevelopmentSchemaArns",
        "clouddirectory:ListDirectories",
        "clouddirectory:ListPublishedSchemaArns",
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "cloudfront:List*",
        "cloudhsm:ListAvailableZones",
        "cloudhsm:ListHapgs",
        "cloudhsm:ListHsms",
        "cloudhsm:ListLunaClients",
        "cloudsearch:DescribeDomains",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codebuild:ListBuilds*",
        "codebuild:ListProjects",
        "codecommit:List*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:ListPipelines",
        "codestar:List*",
        "cognito-identity:ListIdentities",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:List*",
        "cognito-sync:ListDatasets",
        "config:Describe*",
        "config:List*",
        "connect:List*",
        "comprehend:Describe*",
        "comprehend:List*",
        "datapipeline:DescribePipelines",
        "datapipeline:GetAccountLimits",
        "datapipeline:ListPipelines",
        "dax:DescribeClusters",
        "dax:DescribeDefaultParameters",
```

```
        "dax:DescribeEvents",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "devicefarm:List*",
        "directconnect:Describe*",
        "discovery:List*",
        "dms:List*",
        "ds:DescribeDirectories",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListBackups",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeBundleTasks",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeHost*",
        "ec2:DescribeIdFormat",
        "ec2:DescribeIdentityIdFormat",
        "ec2:DescribeImage*",
        "ec2:DescribeImport*",
        "ec2:DescribeInstance*",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
```

```
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetwork*",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeReserved*",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshot*",
        "ec2:DescribeSpot*",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolume*",
        "ec2:DescribeVpc*",
        "ec2:DescribeVpnGateways",
        "ec2:SearchLocalGatewayRoutes",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:Describe*",
        "ecs:List*",
        "elastic-inference:DescribeAccelerators",
        "elastic-inference:DescribeAcceleratorTypes",
        "elastic-inference:DescribeAcceleratorOfferings",
        "elastic-inference:ListTagsForResource",
        "elasticache:Describe*",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticbeanstalk:ListAvailableSolutionStacks",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:List*",
```

```
        "elastictranscoder:List*",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:ListDomainNames",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "firehose:DescribeDeliveryStream",
        "firehose:List*",
        "fsx:DescribeFileSystems",
        "gamelift:List*",
        "glacier:List*",
        "greengrass:List*",
        "iam:GetAccountSummary",
        "iam:GetLoginProfile",
        "iam:List*",
        "importexport:ListJobs",
        "inspector:List*",
        "iot:List*",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kms:ListKeys",
        "lambda:List*",
        "lex:GetBotAliases",
        "lex:GetBotChannelAssociations",
        "lex:GetBotVersions",
        "lex:GetBots",
        "lex:GetIntentVersions",
        "lex:GetIntents",
        "lex:GetSlotTypeVersions",
        "lex:GetSlotTypes",
        "lex:GetUtterancesView",
        "lightsail:GetBlueprints",
        "lightsail:GetBundles",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetRegions",
        "lightsail:GetStaticIps",
        "lightsail:IsVpcPeered",
        "logs:Describe*",
        "lookoutvision:ListModelPackagingJobs",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
```

```
        "machinelearning:Describe*",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetImportJobs",
        "mobiletargeting:GetSegments",
        "opsworks-cm:Describe*",
        "opsworks:Describe*",
        "organizations:List*",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites",
        "outposts:ListTagsForResource",
        "polly:Describe*",
        "polly:List*",
        "rds:Describe*",
        "redshift:DescribeClusters",
        "redshift:DescribeEvents",
        "redshift:ViewQueriesInConsole",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "route53:Get*",
        "route53:List*",
        "route53domains:List*",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sdb:List*",
        "servicecatalog:List*",
        "ses:List*",
        "shield:List*",
        "sns:List*",
        "sqs:ListQueues",
```

```
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "states:ListActivities",
        "states:ListStateMachines",
        "storagegateway:ListGateways",
        "storagegateway:ListLocalDisks",
        "storagegateway:ListVolumeRecoveryPoints",
        "storagegateway:ListVolumes",
        "swf:List*",
        "trustedadvisor:Describe*",
        "waf-regional:List*",
        "waf:List*",
        "wafv2:List*",
        "workdocs:DescribeAvailableDirectories",
        "workdocs:DescribeInstances",
        "workmail:Describe*",
        "workspaces:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

VMImportExportRoleForAWSConnector

`VMImportExportRoleForAWSConnector`adalah kebijakanAWS terkelola yang: Kebijakan default untuk peran layanan Impor/Ekspor VM, untuk pelanggan yang menggunakanAWS Konektor. Layanan Impor/Ekspor VM berperan dengan kebijakan ini untuk memenuhi permintaan migrasi mesin virtual dari alat virtualAWS Connector. (Perhatikan bahwaAWS Connector menggunakan "AWSConnector" kebijakan terkelola untuk mengeluarkan permintaan atas nama pelanggan ke layanan VM Import Impor/Ekspor.) Memberikan kemampuan untuk membuat snapshot AMI dan EBS,

memodifikasi atribut snapshot EBS, membuat panggilan “Jelaskan*” pada objek EC2, dan membaca dari bucket S3 dimulai dengan 'import-to-ec2-'.

Menggunakan kebijakan ini

Anda dapat melampirkan`VMImportExportRoleForAWSConnector` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: Kebijakan peran layanan
- Waktu pembuatan: 03 September 2015, 20:48 UTC
- Waktu yang telah diedit: 03 September 2015 08.48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::import-to-ec2-*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:CopySnapshot",
        "ec2:RegisterImage",
        "ec2:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas identitas identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

VPCLatticeFullAccess

`VPCLatticeFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh ke Amazon VPC Lattice dan akses ke layanan dependensi.

Menggunakan kebijakan ini

Anda dapat melampirkan`VPCLatticeFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 Maret 2023, 02:49 UTC
- Waktu yang telah diedit: 30 Maret 2023, 02:49 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "logs:DescribeLogGroups",
        "s3:ListAllMyBuckets",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
```

```
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:UpdateLogDelivery",
        "logs:DescribeResourcePolicies"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "vpc-lattice.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "delivery.logs.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice"
```

```
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

VPCLatticeReadOnlyAccess

`VPCLatticeReadOnlyAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses hanya-baca ke Amazon VPC Lattice melaluiAWS Management Console, dan akses terbatas ke layanan dependensi.

Menggunakan kebijakan ini

Anda dapat melampirkan`VPCLatticeReadOnlyAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 Maret 2023, 02:47 UTC
- Waktu yang telah diedit: 30 Maret 2023, 02:47 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:Get*",
        "vpc-lattice:List*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "logs:DescribeLogGroups",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

VPCLatticeServicesInvokeAccess

`VPCLatticeServicesInvokeAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses untuk menerapkan layanan Amazon VPC Lattice.

Menggunakan kebijakan ini

Anda dapat melampirkan`VPCLatticeServicesInvokeAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan kebijakan kebijakan kebijakan kebijakan kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 30 Maret 2023, 02:45 UTC
- Waktu yang telah diedit: 30 Maret 2023, 02:45 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice-svcs:Invoke"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

WAFLoggingServiceRolePolicy

`WAFLoggingServiceRolePolicy`adalah kebijakanAWS terkelola yang: Membuat SLR untuk menulis log pelanggan ke aliran firehose

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, atau peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 Agustus 2018, 21:05 UTC
- Waktu yang telah diedit: 24 Agustus 2018 09.05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan tersebut. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa

WAFRegionalLoggingServiceRolePolicy

`WAFRegionalLoggingServiceRolePolicy`adalah kebijakanAWS terkelola yang: Membuat SLR untuk menulis log pelanggan ke aliran firehose

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna,,,,, tidak dapat dilampirkan kebijakan ini.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 24 Agustus 2018, 18:40 UTC
- Waktu yang telah diedit: 24 Agustus 2018 06.40 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

WAFV2LoggingServiceRolePolicy

`WAFV2LoggingServiceRolePolicy`adalah kebijakanAWS terkelola yang: Kebijakan ini membuat peran terkait layanan yang memungkinkanAWS WAF menulis log ke Amazon Kinesis Data Firehose.

Menggunakan kebijakan ini

Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan layanan untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke peran Anda tidak dapat melampirkan kebijakan ini ke peran Anda.

Rincian kebijakan

- Tipe: Kebijakan peran terkait layanan
- Waktu pembuatan: 07 November 2019, 00:40 UTC
- Waktu yang telah diedit: 23 Juli 2020, 17.04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v2 (default)

Versi default kebijakan ini adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

WellArchitectedConsoleFullAccess

`WellArchitectedConsoleFullAccess`adalah kebijakanAWS terkelola yang: Menyediakan akses penuh keAWS Well-Architected Tool melaluiAWS Management Console

Menggunakan kebijakan ini

Anda dapat melampirkan`WellArchitectedConsoleFullAccess` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 29 November 2018, 18:19 UTC
- Waktu yang telah diedit: 29 November 2018 08.19 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

WellArchitectedConsoleReadOnlyAccess

`WellArchitectedConsoleReadOnlyAccess`adalah kebijakan AWS terkelola yang: Menyediakan akses hanya-baca ke AWS Well-Architected Tool melalui AWS Management Console

Menggunakan kebijakan ini

Anda dapat melampirkan `WellArchitectedConsoleReadOnlyAccess` ke pengguna, grup, dan peran Anda.

Rincian kebijakan

- Jenis: kebijakan AWS terkelola
- Waktu pembuatan: 29 November 2018, 18:21 UTC
- Waktu yang telah diedit: 29 Juni 2023, 17.16 UTC

- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

Versi kebijakan

Versi kebijakan: v2 (default)

Versi default kebijakan adalah versi yang mendefinisikan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengakses AWS sumber daya, AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:Get*",
        "wellarchitected:List*",
        "wellarchitected:ExportLens"
      ],
      "Resource" : "*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakan AWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakan AWS terkelola dan beralih ke izin paling sedikit hak istimewa

WorkLinkServiceRolePolicy

`WorkLinkServiceRolePolicy`adalah kebijakanAWS terkelola yang: Memungkinkan akses keLayanan AWS dan Sumber Daya yang digunakan atau dikelola oleh Amazon WorkLink

Menggunakan kebijakan ini

Anda dapat melampirkan`WorkLinkServiceRolePolicy` ke pengguna, grup, dan peran Anda.

detail kebijakan

- Jenis: kebijakanAWS terkelola
- Waktu pembuatan: 23 Januari 2019, 19:03 UTC
- Waktu yang telah diedit: 23 Januari 2019 19.03 UTC
- ARN: `arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy`

Versi kebijakan

Versi kebijakan:v1 (default)

Versi default kebijakan adalah versi yang menentukan izin untuk kebijakan. Ketika pengguna atau peran dengan kebijakan membuat permintaan untuk mengaksesAWS sumber daya,AWS periksa versi default kebijakan untuk menentukan apakah akan mengizinkan permintaan.

Dokumen kebijakan JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords"
```

```
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/AmazonWorkLink-*"
    }
  ]
}
```

Pelajari selengkapnya

- Membuat set izin menggunakan kebijakanAWS terkelola di IAM Identity Center
- Menambahkan dan menghapus izin identitas IAM
- Memahami versi untuk kebijakan IAM
- Memulai kebijakanAWS terkelola dan beralih ke izin paling tidak memiliki hak istimewa

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.