aws

リファレンスガイド

AWS マネージドポリシー

AWS マネージドポリシー: リファレンスガイド

Table of Contents

AWS マネージドポリシーとは何ですか?

AWS マネージドポリシーは、AWS が作成および管理するスタンドアロンポリシーです。AWS マネージドポリシーは、多くの一般的なユースケースでアクセス許可を提供できるように設計されています。これにより、自身でポリシーを記述するよりも簡単に、ユーザー、グループ、ロールに許可を割り当てることができます。

AWS マネージドポリシーは、すべての AWS のユーザーが使用できるため、特定のユースケースに対して最小特権のアクセス許可が付与されない場合があることに留意してください。ユースケース別にカスタマーマネージドポリシーを定義することで、アクセス許可を絞り込むことをお勧めします。

AWS マネージドポリシーで定義したアクセス権限は変更できません。AWS が AWS マネージドポリシーに定義されているアクセス許可を更新すると、更新はポリシーがアタッチされているすべてのプリンシパルアイデンティティ (ユーザー、グループ、ロール) に影響します。新しい AWS サービスを起動するか、既存のサービスで新しい API オペレーションが使用可能になると、AWS が AWS マネージドポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

ポリシーリファレンスページについて

各ポリシーリファレンスページには、以下の情報が含まれています。

- このポリシーを使用すると — ユーザー、グループ、ロールにポリシーをアタッチできるかどうか
- ポリシーの詳細
  - タイプ — AWS マネージドポリシーのタイプ
    - `AWS managed policy` — 標準 AWS マネージドポリシー
    - `Job function policy` — 一般的な業界職務に沿ったポリシー
    - `Service-linked role policy` — ユーザーに代わって the section called “AmazonRDSPreviewServiceRolePolicy” のようなアクションを実行することをサービスに許可する、サービスリンクロールにアタッチするポリシー
    - `Service role policy` — the section called “AWSControlTowerServiceRolePolicy” のようなサービスロールと連携するように設計されたポリシー
  - 作成日時 — ポリシーが最初に作成された日時
  - 編集日時 — このバージョンのポリシーが編集された日時

  - ARN — ポリシーの Amazon リソースネーム
- ポリシーのバージョン — ポリシーによって付与された許可バージョン
- JSON ポリシードキュメント — ポリシー JSON
- 詳細 — AWS マネージドポリシーに関連するドキュメントへのリンク

非推奨の AWS マネージドポリシー

AWS は、AWS マネージドポリシーを定期的に更新します。ほとんどの場合、アクセス許可をポリシーに追加します。これは、新しいサービスや機能をリリースしたときに行われます。AWS マネージドポリシーのセキュリティを向上させるために、ポリシーの範囲を縮小することがあります。ポリシーからアクセス許可を削除すると、ポリシーを非推奨の状態に設定し、新しいポリシーを利用できるようにします。AWS がサービスまたは機能を廃止すると、その機能の AWS マネージドポリシーも廃止されます。

使用しているポリシーが廃止されたというメール通知を受け取った場合は、直ちに対応することをお勧めします。ポリシーの変更を特定し、ワークフローを更新してください。AWS が交換ポリシーを提供する場合、影響を受けるすべてのアイデンティティ (ユーザー、グループ、およびロール) にそのポリシーをアタッチした後、それらのアイデンティティから廃止されたポリシーをデタッチします。

非推奨のポリシーには以下のような特徴があります。

- このガイドからは削除されています。
- アクセス許可は、現在アタッチされているすべてのアイデンティティに対して引き続き機能します。
- ポリシーがアイデンティティにアタッチされているアカウントでは、IAM コンソールの [Policies] リストに警告アイコンと共に表示されます。
- 新しいアイデンティティにはアタッチできません。現在のアイデンティティからポリシーをデタッチした場合、再アタッチすることはできません。
- 現在のすべてのエンティティからポリシーをデタッチしたら、そのポリシーは表示されなくなります。

AWS マネージドポリシー

AWS マネージドポリシー

- 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` は、Access Analyzer にリソースのメタデータを分析することを許可する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 2 日 17:13 UTC
- 編集日時： 2024 年 1 月 22 日 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v12 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AdministratorAccess

AdministratorAccess は、 AWS サービスとリソースへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AdministratorAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2015 年 2 月 6 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AdministratorAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AdministratorAccess-Amplify

`AdministratorAccess-Amplify` は、Amplify アプリケーションが必要とするリソースへの直接アクセスを明示的に許可し、アカウントに管理権限を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AdministratorAccess-Amplify` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 1 日 19:03 UTC
- 編集日時: 2023 年 5 月 31 日 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-Amplify`

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AdministratorAccess-AWSElasticBeanstalk

`AdministratorAccess-AWSElasticBeanstalk` は、アカウントに管理権限を付与する AWS マネージドポリシーです。開発者や管理者が AWS Elastic Beanstalk アプリケーションの管理に必要なリソースに直接アクセスすることを明示的に許可します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AdministratorAccess-AWSElasticBeanstalk` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 1 月 22 日 19:36 UTC
- 編集日時: 2023 年 3 月 23 日 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AlexaForBusinessDeviceSetup

`AlexaForBusinessDeviceSetup` は、AlexaforBusiness サービスへのデバイス設定アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AlexaForBusinessDeviceSetup` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 30 日 16:47 UTC
- 編集日時: 2019 年 5 月 20 日 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    }
```

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AlexaForBusinessFullAccess

`AlexaForBusinessFullAccess` は、AlexaForBusiness リソースへのフルアクセスと関連 AWS のサービス へのアクセス権を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AlexaForBusinessFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 30 日 16:47 UTC
- 編集日時: 2020 年 7 月 1 日 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "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*"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AlexaForBusinessGatewayExecution

`AlexaForBusinessGatewayExecution` は、AlexaforBusiness サービスへのゲートウェイ実行アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AlexaForBusinessGatewayExecution` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 30 日 16:47 UTC
- 編集日時: 2017 年 11 月 30 日 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
```

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AlexaForBusinessLifesizeDelegatedAccessPolicy

`AlexaForBusinessLifesizeDelegatedAccessPolicy` は、Lifesize AVS デバイスへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AlexaForBusinessLifesizeDelegatedAccessPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 6 月 4 日 19:46 UTC
- 編集日時: 2020 年 6 月 12 日 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AlexaForBusinessNetworkProfileServicePolicy

`AlexaForBusinessNetworkProfileServicePolicy` は、Alexa for Business はネットワークプロファイルによってスケジュールされた自動タスクを実行可能にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 3 月 13 日 00:53 UTC
- 編集日時: 2019 年 4 月 5 日 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AlexaForBusinessPolyDelegatedAccessPolicy

AlexaForBusinessPolyDelegatedAccessPolicy は、Poly AVS デバイスへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AlexaForBusinessPolyDelegatedAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 10 月 16 日 19:48 UTC
- 編集日時: 2019 年 10 月 16 日 19:48 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AlexaForBusinessReadOnlyAccess

`AlexaForBusinessReadOnlyAccess` は、AlexaForBusiness サービスへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AlexaForBusinessReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 30 日 16:47 UTC

- 編集日時: 2019 年 11 月 20 日 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonAPIGatewayAdministrator

AmazonAPIGatewayAdministrator は、AWS Management Console を使用して Amazon API Gateway で API を作成/編集/削除するためのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAPIGatewayAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 7 月 9 日 17:34 UTC
- 編集日時: 2015 年 7 月 9 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonAPIGatewayInvokeFullAccess

`AmazonAPIGatewayInvokeFullAccess` は、Amazon API Gateway で API を呼び出すためのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonAPIGatewayInvokeFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 7 月 9 日 17:36 UTC
- 編集日時: 2018 年 12 月 18 日 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonAPIGatewayPushToCloudWatchLogs

AmazonAPIGatewayPushToCloudWatchLogs は、API Gateway がユーザーのアカウントにログをプッシュできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAPIGatewayPushToCloudWatchLogs をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 11 月 11 日 23:41 UTC
- 編集日時: 2015 年 11 月 11 日 23:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonAppFlowFullAccess

AmazonAppFlowFullAccess は、Amazon AppFlow へのフルアクセスと、フローの送信元または送信先としてサポートされている AWS サービス (S3 および Redshift) へのアクセスを提供する AWS マネージドポリシーです。また、KMS にアクセスして暗号化することもできます。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAppFlowFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 6 月 2 日 23:30 UTC
- 編集日時: 2022 年 2 月 28 日 23:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAppFlowFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonAppFlowReadOnlyAccess

`AmazonAppFlowReadOnlyAccess` は、Amazon Appflow フローへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonAppFlowReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 6 月 2 日 23:26 UTC
- 編集日時: 2022 年 2 月 28 日 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonAppStreamFullAccess

AmazonAppStreamFullAccess は、AWS Management Console 経由で Amazon AppStream へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAppStreamFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2020 年 8 月 28 日 17:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAppStreamFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonAppStreamPCAAccess

AmazonAppStreamPCAAccess は、Amazon AppStream 2.0 が顧客アカウント内の AWS Certificate Manager Private CA にアクセスして証明書ベースの認証を可能にする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAppStreamPCAAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 24 日 17:05 UTC

- 編集日時: 2022 年 10 月 24 日 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonAppStreamReadOnlyAccess

AmazonAppStreamReadOnlyAccess は、AWS Management Console 経由で Amazon AppStream への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAppStreamReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2016 年 12 月 7 日 21:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonAppStreamServiceAccess

`AmazonAppStreamServiceAccess` は、Amazon AppStream サービスロールのデフォルトポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonAppStreamServiceAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 11 月 19 日 04:17 UTC
- 編集日時: 2020 年 6 月 26 日 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonAthenaFullAccess

AmazonAthenaFullAccess は、Amazon Athena へのフルアクセスと、クエリ、結果の書き込み、データ管理に必要な依存関係へのスコープ付きアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAthenaFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 11 月 30 日 16:46 UTC
- 編集日時： 2024 年 1 月 3 日 19:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAthenaFullAccess

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonAugmentedAIFullAccess

`AmazonAugmentedAIFullAccess` は、FlowDefinition、HumanTaskUi、HumanLoop など、Amazon Augmented AI リソースのすべてのオペレーションを実行するためのアクセスを提供する AWS マネージドポリシーです。一般公開のワークチームに対する FlowDefinition の作成にはアクセスできません。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonAugmentedAIFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 3 日 16:21 UTC
- 編集日時: 2019 年 12 月 3 日 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
```

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonAugmentedAIHumanLoopFullAccess

AmazonAugmentedAIHumanLoopFullAccess は、HumanLoops のすべてのオペレーションを実行するためのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAugmentedAIHumanLoopFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 3 日 16:20 UTC
- 編集日時: 2019 年 12 月 3 日 16:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonAugmentedAIIntegratedAPIAccess

`AmazonAugmentedAIIntegratedAPIAccess` は、FlowDefinition、HumanTaskUi、HumanLoop など、Amazon Augmented AI リソースのすべてのオペレーションを実行するためのアクセスを提供する AWS マネージドポリシーです。また、Amazon Augmented AI と統合されたサービスの運用にもアクセスできます。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonAugmentedAIIntegratedAPIAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2020 年 4 月 22 日 20:47 UTC
- 編集日時: 2020 年 4 月 22 日 20:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonBedrockFullAccess

`AmazonBedrockFullAccess`は、Amazon Bedrock へのフルアクセスと、Amazon Bedrock AWSが必要とする関連サービスへの制限付きアクセスを提供する管理ポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonBedrockFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時間:2023 年 12 月 6 日 15:47 UTC
- 編集時間:2023 年 12 月 6 日 15:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBedrockFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonBedrockReadOnly

AmazonBedrockReadOnlyは、Amazon Bedrock AWSへの読み取り専用アクセスを提供する管理ポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonBedrockReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時間:2023 年 12 月 6 日 15:48 UTC
- 編集時間:2023 年 12 月 6 日 15:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBedrockReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonBraketFullAccess

`AmazonBraketFullAccess` は、AWS Management Console および SDK を使用して Amazon Braket へのフルアクセスを提供する AWS マネージドポリシーです。関連サービス (S3、ログなど) へのアクセスも提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonBraketFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 8 月 6 日 20:12 UTC
- 編集日時: 2023 年 4 月 19 日 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonBraketJobsExecutionPolicy

AmazonBraketJobsExecutionPolicy は、S3、Cloudwatch、IAM、Braket など、Amazon Braket ジョブの実行に必要な AWS のサービス およびリソースへのアクセス権を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonBraketJobsExecutionPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 26 日 19:34 UTC
- 編集日時: 2021 年 11 月 28 日 05:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonBraketServiceRolePolicy

`AmazonBraketServiceRolePolicy` は、Amazon Braket がユーザーに代わって AWS リソースを作成し管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 8 月 4 日 17:12 UTC
- 編集日時: 2020 年 8 月 6 日 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonChimeFullAccess

AmazonChimeFullAccess は、AWS Management Console 経由で Amazon Chime 管理コンソールへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonChimeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 1 日 22:15 UTC
- 編集日時: 2020 年 12 月 14 日 21:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
      ]
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonChimeReadOnly

`AmazonChimeReadOnly` は、AWS Management Console 経由で Amazon Chime 管理コンソールへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonChimeReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 1 日 22:04 UTC
- 編集日時: 2020 年 12 月 14 日 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonChimeSDK

AmazonChimeSDK は、Amazon Chime SDK オペレーションへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonChimeSDK をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 2 月 4 日 21:53 UTC
- 編集日時: 2023 年 1 月 10 日 18:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeSDK

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicyは、AWS Amazon Chime SDK MediaPipelines サービスにリンクされたロールの管理ポリシーとなる管理ポリシーです

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 4 月 4 日 22:02 UTC
- 編集時間:2023 年 12 月 8 日 19:14 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonChimeSDKMessagingServiceRolePolicy

AmazonChimeSDKMessagingServiceRolePolicy は、Amazon Chime SDK Messaging が AWS リソースにアクセスし、メッセージング機能を有効化できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 3 月 3 日 01:43 UTC

- 編集日時: 2023 年 3 月 3 日 01:43 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
      ]
```

```
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonChimeServiceRolePolicy

AmazonChimeServiceRolePolicy は、Amazon Chime が使用または管理する AWS リソースへのアクセスを有効にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 9 月 30 日 22:25 UTC
- 編集日時: 2019 年 9 月 30 日 22:25 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonChimeTranscriptionServiceLinkedRolePolicy

AmazonChimeTranscriptionServiceLinkedRolePolicy は、Amazon Chime がユーザーに代わって Amazon Transcribe および Amazon Transcribe Medical にアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 8 月 4 日 21:47 UTC
- 編集日時: 2021 年 8 月 4 日 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonChimeUserManagement

AmazonChimeUserManagement は、AWS Management Console 経由で Amazon Chime 管理コンソールへのユーザー管理アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonChimeUserManagement をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 1 日 22:17 UTC
- 編集日時: 2020 年 2 月 18 日 19:26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeUserManagement

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

AmazonChimeVoiceConnectorServiceLinkedRolePolicy は、Amazon Chime VoiceConnector のサービスリンクロールのマネージドポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 9 月 30 日 22:16 UTC
- 編集日時: 2023 年 4 月 14 日 21:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCloudDirectoryFullAccess

AmazonCloudDirectoryFullAccess は、Amazon Cloud Directory サービスへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCloudDirectoryFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 2 月 25 日 00:41 UTC
- 編集日時: 2017 年 2 月 25 日 00:41 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCloudDirectoryReadOnlyAccess

`AmazonCloudDirectoryReadOnlyAccess` は、Amazon Cloud Directory サービスへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCloudDirectoryReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 2 月 28 日 23:42 UTC
- 編集日時: 2017 年 2 月 28 日 23:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCloudWatchEvidentlyFullAccess

`AmazonCloudWatchEvidentlyFullAccess` は、Amazon CloudWatch Evidently へのフルアクセスのみを提供する AWS マネージドポリシーです。関連する Amazon S3、Amazon SNS、Amazon CloudWatch およびその他の関連サービスへのアクセスも提供されます。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCloudWatchEvidentlyFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 29 日 15:10 UTC
- 編集日時: 2021 年 11 月 29 日 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCloudWatchEvidentlyReadOnlyAccess

`AmazonCloudWatchEvidentlyReadOnlyAccess` は、Amazon CloudWatch Evidently への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCloudWatchEvidentlyReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 29 日 15:08 UTC
- 編集日時: 2021 年 11 月 29 日 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCloudWatchEvidentlyServiceRolePolicy

AmazonCloudWatchEvidentlyServiceRolePolicy は、CloudWatch Evidently サービスがお客様に代わって関連する AWS リソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 9 月 13 日 17:25 UTC
- 編集日時: 2022 年 9 月 13 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCloudWatchRUMFullAccess

`AmazonCloudWatchRUMFullAccess` は、Amazon CloudWatch RUM サービスにフルアクセス権を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCloudWatchRUMFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 29 日 15:46 UTC
- 編集日時: 2021 年 11 月 29 日 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCloudWatchRUMReadOnlyAccess

AmazonCloudWatchRUMReadOnlyAccess は、Amazon CloudWatch RUM サービスに読み取り専用のアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCloudWatchRUMReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 29 日 15:43 UTC
- 編集日時: 2022 年 10 月 28 日 18:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCloudWatchRUMServiceRolePolicy

AmazonCloudWatchRUMServiceRolePolicy は、モニタリングデータを他の関連する AWS サービスに公開するアクセス許可を Amazon CloudWatch RUM サービスに付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 17 日 23:17 UTC
- 編集日時: 2023 年 2 月 22 日 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCodeCatalystFullAccess

`AmazonCodeCatalystFullAccess` は、Amazon CodeCatalyst へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCodeCatalystFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 4 月 20 日 16:50 UTC
- 編集日時: 2023 年 4 月 20 日 16:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCodeCatalystReadOnlyAccess

AmazonCodeCatalystReadOnlyAccess は、Amazon CodeCatalyst への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeCatalystReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 4 月 20 日 16:49 UTC
- 編集日時: 2023 年 4 月 20 日 16:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCodeCatalystSupportAccess

AmazonCodeCatalystSupportAccess は、Amazon CodeCatalyst がお客様に代わって AWS Support ケースを作成、更新、解決できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeCatalystSupportAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 20 日 12:34 UTC
- 編集日時: 2023 年 4 月 20 日 12:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCodeGuruProfilerAgentAccess

AmazonCodeGuruProfilerAgentAccess は、Amazon CodeGuru Profiler エージェントが必要とするアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeGuruProfilerAgentAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 2 月 5 日 22:11 UTC
- 編集日時: 2022 年 5 月 5 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:ConfigureAgent",
        "codeguru-profiler:CreateProfilingGroup",
        "codeguru-profiler:PostAgentProfile"
      ],
      "Resource" : "arn:aws:codeguru-profiler:*:*:profilingGroup/*"
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCodeGuruProfilerFullAccess

`AmazonCodeGuruProfilerFullAccess` は、Amazon CodeGuru Profiler へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCodeGuruProfilerFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 3 日 10:13 UTC
- 編集日時: 2020 年 7 月 15 日 03:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCodeGuruProfilerReadOnlyAccess

`AmazonCodeGuruProfilerReadOnlyAccess` は、Amazon CodeGuru Profiler への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeGuruProfilerReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 3 日 10:30 UTC
- 編集日時: 2020 年 6 月 27 日 23:52 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCodeGuruReviewerFullAccess

`AmazonCodeGuruReviewerFullAccess` は、Amazon CodeGuru Reviewer へのフルアクセス権と、必要な依存関係へのスコープ付きアクセス権を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCodeGuruReviewerFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 3 日 08:33 UTC
- 編集日時: 2020 年 8 月 29 日 04:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCodeGuruReviewerReadOnlyAccess

AmazonCodeGuruReviewerReadOnlyAccess は、Amazon CodeGuru Reviewer への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeGuruReviewerReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2019 年 12 月 3 日 08:48 UTC
- 編集日時: 2020 年 8 月 29 日 04:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCodeGuruReviewerServiceRolePolicy

AmazonCodeGuruReviewerServiceRolePolicy は、Amazon CodeGuru Reviewer がユーザーに代わってリソースにアクセスするために必要なサービスリンクロールである AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 3 日 05:31 UTC
- 編集日時: 2020 年 11 月 27 日 15:09 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*/*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCodeGuruSecurityFullAccess

`AmazonCodeGuruSecurityFullAccess` は、Amazon CodeGuru Security へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeGuruSecurityFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 5 月 9 日 21:03 UTC
- 編集日時: 2023 年 5 月 9 日 21:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCodeGuruSecurityScanAccess

AmazonCodeGuruSecurityScanAccess は、Amazon CodeGuru Security スキャンの操作に必要なアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeGuruSecurityScanAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 5 月 9 日 20:54 UTC
- 編集日時: 2023 年 5 月 9 日 20:54 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCognitoDeveloperAuthenticatedIdentities

`AmazonCognitoDeveloperAuthenticatedIdentities` は、Amazon Cognito API へのアクセスを提供して、認証バックエンドからの開発者認証アイデンティティをサポートする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCognitoDeveloperAuthenticatedIdentities` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 3 月 24 日 17:22 UTC
- 編集日時: 2015 年 3 月 24 日 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCognitoIdpEmailServiceRolePolicy

`AmazonCognitoIdpEmailServiceRolePolicy` は、Amazon Cognito ユーザープールサービスが E メール送信に SES アイデンティティを使用できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 3 月 21 日 21:32 UTC
- 編集日時: 2019 年 3 月 21 日 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCognitoIdpServiceRolePolicy

AmazonCognitoIdpServiceRolePolicy は、Amazon Cognito ユーザープールが使用または管理する AWS のサービス およびリソースへのアクセスを有効にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 6 月 26 日 22:30 UTC
- 編集日時: 2020 年 6 月 26 日 22:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCognitoPowerUser

AmazonCognitoPowerUser は、既存の Amazon Cognito リソースへの管理アクセスを提供する AWS マネージドポリシーです。新しい Cognito リソースを作成するには、AWS アカウント 管理者権限が必要です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCognitoPowerUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 3 月 24 日 17:14 UTC
- 編集日時: 2021 年 6 月 1 日 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoPowerUser

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCognitoReadOnly

AmazonCognitoReadOnly は、Amazon Cognito リソースへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCognitoReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 3 月 24 日 17:06 UTC
- 編集日時: 2019 年 8 月 1 日 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
```

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCognitoUnAuthedIdentitiesSessionPolicy

AmazonCognitoUnAuthedIdentitiesSessionPolicy は、Cognito アイデンティティプールの認証されていないアイデンティティに許可されるアクセス許可のセットを定義する AWS マネージドポリシーです。このポリシーは、スタンドアロンのアクセス許可ポリシーとして使用することを意図したものではありません。アイデンティティプール内のロールにアタッチされている過度に許容度の高いポリシーに対するガードレールとして使用されます。このポリシーはどのロールにもアタッチしないでください。Cognito Identity Service は、認証情報を作成するときに、このポリシーをスコープダウンポリシーとして自動的に含めます。拡張フローを通じて他の AWS リソースに一時的にアクセスする権限は、サービスによって提供される認証されていないユーザーのアイデンティティに関連付けられたロールと、Cognito が所有するこのマネージドポリシーで与えられる権限の共通部分によって定義されるようになります。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCognitoUnAuthedIdentitiesSessionPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 7 月 19 日 23:04 UTC
- 編集日時: 2023 年 7 月 19 日 23:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonCognitoUnauthenticatedIdentities

AmazonCognitoUnauthenticatedIdentities は、Cognito アイデンティティプールの認証されていないアイデンティティに許可されるアクセス許可のセットを定義する AWS マネージドポリシーです。これを unauth ロールにアタッチする必要はありません。Cognito Identity Service は、認証情報を作成するときに、このロールをスコープダウンポリシーとして自動的に含めます。拡張フローを通じて他の AWS リソースに一時的にアクセスする権限は、サービスによって提供される認証されていないユーザーのアイデンティティに関連付けられたロールと、Cognito が所有するこのマネージドポリシーで与えられる権限の共通部分によって定義されるようになります。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCognitoUnauthenticatedIdentities をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 2 月 1 日 22:36 UTC
- 編集日時: 2023 年 2 月 1 日 22:36 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonConnect_FullAccess

AmazonConnect_FullAccess は、Connect リソースを使用するために必要なアクセス許可を AWS Connect ユーザーに付与するための AWS マネージドポリシーです。このポリシーは、Connect Console とパブリック API を介して AWS Connect リソースへのフルアクセスを提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonConnect_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 11 月 20 日 19:54 UTC
- 編集日時: 2023 年 3 月 7 日 14:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonConnect_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonConnectCampaignsServiceLinkedRolePolicy

`AmazonConnectCampaignsServiceLinkedRolePolicy` は、Amazon Connect キャンペーンのサービスリンクロールに関するポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 9 月 23 日 20:54 UTC
- 編集日時: 2023 年 11 月 8 日 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonConnectReadOnlyAccess

AmazonConnectReadOnlyAccess は、AWS アカウント 内で Amazon Connect インスタンスを表示するアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonConnectReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 10 月 17 日 21:00 UTC
- 編集日時: 2019 年 11 月 6 日 22:10 UTC
- ARN: arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonConnectServiceLinkedRolePolicy

`AmazonConnectServiceLinkedRolePolicy` は、Amazon Connect がユーザーに代わって AWS リソースを作成および管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2018 年 9 月 7 日 00:21 UTC
- 編集時間:2023 年 11 月 28 日 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonConnectSynchronizationServiceRolePolicy

AmazonConnectSynchronizationServiceRolePolicy は、Amazon Connect がユーザーに代わってリージョン間で AWS リソースを同期できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 10 月 27 日 22:38 UTC
- 編集日時: 2023 年 10 月 27 日 22:38 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonConnectVoiceIDFullAccess

AmazonConnectVoiceIDFullAccess は、Amazon Connect Voice ID へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonConnectVoiceIDFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 9 月 26 日 19:04 UTC
- 編集日時: 2021 年 9 月 26 日 19:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDataZoneDomainExecutionRolePolicy

AmazonDataZoneDomainExecutionRolePolicy は、Amazon DomainExecutionRole のサービスロールのデフォルトポリシーである AWS マネージドポリシー DataZoneです。このロールは、Amazon DataZone ドメイン内のデータのカタログ化、検出、管理、共有、分析 DataZone を行うために Amazon によって使用されます。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneDomainExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 9 月 27 日 21:55 UTC
- 編集日時： 2024 年 3 月 12 日 23:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonDataZoneEnvironmentRolePermissionsBoundary

AmazonDataZoneEnvironmentRolePermissionsBoundaryは、Amazon がデータ分析アクションを実行するための Environments 用の IAM DataZone ロールを作成し、AWSこれらのロールを作成する際にこのポリシーを使用して権限の境界を定義するという管理ポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneEnvironmentRolePermissionsBoundary をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 9 月 11 日 23:38 UTC
- 編集時間:2023 年 11 月 17 日 23:29 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDataZoneFullAccess

`AmazonDataZoneFullAccess` は、経由で Amazon へのフルアクセス DataZone AWS Management Console と、それに必要な関連サービスへの制限付きアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDataZoneFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 9 月 22 日 20:06 UTC
- 編集日時： 2024 年 3 月 12 日 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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_*"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonDataZoneFullUserAccess

`AmazonDataZoneFullUserAccess` は、Amazon へのフルアクセスを提供しますが DataZone、ドメイン、ユーザー、または関連アカウントの管理は許可しない AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneFullUserAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 9 月 22 日 21:06 UTC
- 編集日時： 2024 年 3 月 12 日 23:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonDataZoneGlueManageAccessRolePolicy

AmazonDataZoneGlueManageAccessRolePolicyは、AWS次のような管理ポリシーです。このポリシーは、Amazon DataZone が出版を有効にする権限を付与し、データへのアクセス許可を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneGlueManageAccessRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 9 月 22 日 20:21 UTC
- 編集時間:2023 年 12 月 14 日 23:03 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDataZonePortalFullAccessPolicy

AmazonDataZonePortalFullAccessPolicy は、Amazon DataZone API へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZonePortalFullAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 3 月 26 日 18:24 UTC
- 編集日時: 2023 年 3 月 26 日 18:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDataZonePreviewConsoleFullAccess

AmazonDataZonePreviewConsoleFullAccess は、AWS Management Console 経由で Amazon DataZone のプレビューリリースへのフルアクセスを提供する AWS マネージドポリシーです。関連サービスへの限定アクセスも提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZonePreviewConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 3 月 28 日 15:16 UTC
- 編集日時: 2023 年 7 月 13 日 18:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDataZoneProjectDeploymentPermissionsBoundary

AmazonDataZoneProjectDeploymentPermissionsBoundary は、Amazon DataZone がデータ分析プロジェクトのデプロイに使用する IAM ロールを作成する AWS マネージドポリシーです。DataZone はこれらのロールを作成する際にこのポリシーを使用してアクセス許可の境界を定義します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneProjectDeploymentPermissionsBoundary をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 3 月 21 日 02:54 UTC
- 編集日時: 2023 年 4 月 4 日 02:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneProjectDeploymentPermissionsBoundary

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDataZoneProjectRolePermissionsBoundary

AmazonDataZoneProjectRolePermissionsBoundary は、Amazon DataZone がデータ分析アクションを実行するプロジェクト用の IAM ロールを作成し、これらのロールを作成する際に使用して、アクセス許可の境界を定義するための AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneProjectRolePermissionsBoundary をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 3 月 21 日 02:51 UTC
- 編集日時: 2023 年 3 月 21 日 02:51 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDataZoneRedshiftGlueProvisioningPolicy

AmazonDataZoneRedshiftGlueProvisioningPolicy は、Amazon DataZone がデータのカタログ化、検出、管理、共有、分析を可能にするデータ管理サービスである AWS マネージドポリシーです。Amazon を使用すると DataZone、アカウントおよびサポートされているリージョン間でデータを共有してアクセスできます。Amazon は、Amazon Redshift、Amazon Athena、 AWS Glue、 AWS Lake Formation など、 AWS サービス全体のエクスペリエンス DataZone を簡素化します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneRedshiftGlueProvisioningPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 9 月 22 日 20:19 UTC
- 編集日時： 2024 年 3 月 12 日 16:44 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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*"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonDataZoneRedshiftManageAccessRolePolicy

AmazonDataZoneRedshiftManageAccessRolePolicyは、AWS次のような管理ポリシーです。このポリシーは、Amazon Redshift DataZone データをカタログに公開する権限を Amazon に付与します。また、Amazon Redshift または Amazon Redshift DataZone サーバーレスで公開されているカタログ内のアセットへのアクセスを許可または取り消す権限を Amazon に付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneRedshiftManageAccessRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 9 月 22 日 20:15 UTC

- 編集時間:2023 年 11 月 16 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDetectiveFullAccess

`AmazonDetectiveFullAccess` は、Amazon Detective サービスへのフルアクセスと、コンソール UI の依存関係へのスコープ付きアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDetectiveFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2020 年 4 月 30 日 17:57 UTC
- 編集日時: 2023 年 5 月 17 日 19:39 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDetectiveInvestigatorAccess

`AmazonDetectiveInvestigatorAccess` は、調査員に Amazon Detective サービスへのアクセスと、コンソール UI の依存関係へのスコープ付きアクセスを提供する AWS マネージドポリシーです。このポリシーでは、調査目的で Detective に掘り下げるアクセス許可と、Guardduty への制限付き書き込みアクセス許可を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDetectiveInvestigatorAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 1 月 17 日 15:24 UTC
- 編集時間:2023 年 11 月 27 日 03:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDetectiveMemberAccess

AmazonDetectiveMemberAccess は、Amazon Detective サービスへのメンバーアクセスと、コンソール UI の依存関係へのスコープ付きアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDetectiveMemberAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 1 月 17 日 15:16 UTC
- 編集日時: 2023 年 1 月 17 日 15:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDetectiveOrganizationsAccess

AmazonDetectiveOrganizationsAccess は、Amazon Detective の委任管理者を管理するための Organizations アクセスと、コンソール UI の依存関係へのスコープ付きアクセスを提供する AWS マネージドポリシーです。これにより、Detective のサービスリンクロールを作成するアクセス許可も付与されます。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDetectiveOrganizationsAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 3 月 2 日 15:20 UTC
- 編集日時: 2023 年 3 月 2 日 15:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDetectiveServiceLinkedRolePolicy

AmazonDetectiveServiceLinkedRolePolicy は、Amazon Detective がユーザーに代わってサービス呼び出しを行えるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 18 日 19:47 UTC
- 編集日時: 2021 年 11 月 18 日 19:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDevOpsGuruConsoleFullAccess

AmazonDevOpsGuruConsoleFullAccess は、DevOps Guru コンソールへのフルアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDevOpsGuruConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 12 月 17 日 18:43 UTC
- 編集日時: 2022 年 8 月 25 日 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDevOpsGuruFullAccess

`AmazonDevOpsGuruFullAccess` は、Amazon DevOps Guru へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDevOpsGuruFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 1 日 16:38 UTC
- 編集日時: 2022 年 8 月 25 日 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDevOpsGuruOrganizationsAccess

AmazonDevOpsGuruOrganizationsAccess は、組織内の Amazon DevOps Guru を有効化および管理するためのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDevOpsGuruOrganizationsAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 15 日 23:50 UTC
- 編集日時: 2021 年 11 月 15 日 23:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント


```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDevOpsGuruReadOnlyAccess

AmazonDevOpsGuruReadOnlyAccess は、Amazon DevOps Guru コンソールへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDevOpsGuruReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 1 日 16:34 UTC
- 編集日時: 2022 年 8 月 25 日 18:11 UTC

- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDevOpsGuruServiceRolePolicy

AmazonDevOpsGuruServiceRolePolicy は、Amazon DevOpsGuru がリソースにアクセスする際に必要となる、サービスリンクロールである AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 1 日 10:24 UTC
- 編集日時: 2023 年 1 月 10 日 14:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDMSCloudWatchLogsRole

AmazonDMSCloudWatchLogsRole は、DMS レプリケーションログを顧客アカウントの cloudwatch ログにアップロードするためのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDMSCloudWatchLogsRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 1 月 7 日 23:44 UTC
- 編集日時: 2023 年 5 月 23 日 21:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDMSRedshiftS3Role

AmazonDMSRedshiftS3Role は、DMS の Redshift エンドポイントの S3 設定を管理するためのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDMSRedshiftS3Role をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 4 月 20 日 17:05 UTC
- 編集日時: 2019 年 7 月 8 日 18:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDMSVPCManagementRole

AmazonDMSVPCManagementRole は、AWS 管理対象顧客設定の VPC 設定を管理するためのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDMSVPCManagementRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 11 月 18 日 16:33 UTC
- 編集日時: 2016 年 5 月 23 日 16:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDocDB-ElasticServiceRolePolicy

AmazonDocDB-ElasticServiceRolePolicy は、Amazon DocumentDB-Elastic がユーザーに代わって AWS リソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 30 日 14:17 UTC
- 編集日時: 2022 年 11 月 30 日 14:17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDocDBConsoleFullAccess

`AmazonDocDBConsoleFullAccess` は、AWS Management Console を使用して Amazon DocumentDB (MongoDB 互換) を管理するためのフルアクセスを提供する AWS マネージドポリシーです。このポリシーは、アカウント内のすべての SNS トピックを公開するためのフルアクセス、Amazon EC2 インスタンスと VPC 設定を作成および編集するアクセス許可、Amazon KMS でキーを表示および一覧表示するアクセス許可、Amazon RDS と Amazon Neptune へのフルアクセス権も付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDocDBConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 1 月 9 日 20:37 UTC
- 編集日時: 2022 年 11 月 30 日 15:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDocDBElasticFullAccess

`AmazonDocDBElasticFullAccess` は、Amazon DocumentDB Elastic クラスターへのフルアクセスと、EC2、KMS、SecretsManager、CloudWatch、IAM などの依存関係に必要なその他のアクセス許可を提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDocDBElasticFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 6 月 5 日 13:51 UTC
- 編集日時: 2023 年 6 月 21 日 18:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDocDBElasticReadOnlyAccess

AmazonDocDBElasticReadOnlyAccess は、Amazon DocDB-Elastic と CloudWatch メトリクスへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDocDBElasticReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 6 月 8 日 14:37 UTC

- 編集日時: 2023 年 6 月 21 日 16:57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDocDBFullAccess

AmazonDocDBFullAccess は、Amazon DocumentDB (MongoDB 互換) へのフルアクセスを提供する AWS マネージドポリシーです。このポリシーは、アカウント内のすべての SNS トピックを公開するためのフルアクセスと、Amazon RDS と Amazon Neptune へのフルアクセス権も付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDocDBFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 1 月 9 日 20:21 UTC
- 編集日時: 2019 年 1 月 9 日 20:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDocDBReadOnlyAccess

`AmazonDocDBReadOnlyAccess` は、Amazon DocumentDB (MongoDB 互換) への読み取り専用アクセスを提供する AWS マネージドポリシーです。このポリシーは Amazon RDS と Amazon Neptune リソースへのアクセス権も付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDocDBReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 1 月 9 日 20:30 UTC
- 編集日時: 2019 年 1 月 9 日 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDRSVPCManagement

AmazonDRSVPCManagement は、Amazon が管理する顧客設定の VPC 設定を管理するためのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDRSVPCManagement をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 9 月 2 日 00:09 UTC
- 編集日時: 2015 年 9 月 2 日 00:09 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDRSVPCManagement

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDynamoDBFullAccess

`AmazonDynamoDBFullAccess` は、AWS Management Console 経由で Amazon DynamoDB へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDynamoDBFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2021 年 1 月 29 日 17:38 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess

ポリシーのバージョン

ポリシーのバージョン: v15 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDynamoDBFullAccesswithDataPipeline

`AmazonDynamoDBFullAccesswithDataPipeline` は、廃止予定の AWS マネージドポリシーです。ガイダンスについては、「https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html」のドキュメントを参照してください。AWS Management Console 経由で AWS Data Pipeline を使用したエクスポート/インポートを含む Amazon DynamoDB へのフルアクセスを提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDynamoDBFullAccesswithDataPipeline` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 11 月 12 日 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonDynamoDBReadOnlyAccess

`AmazonDynamoDBReadOnlyAccess` は、経由で Amazon DynamoDB への読み取り専用アクセスを提供する AWS マネージドポリシーです AWS Management Console。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonDynamoDBReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時： 2024 年 3 月 20 日 15:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonEBSCSIDriverPolicy

AmazonEBSCSIDriverPolicy は、CSI ドライバーサービスアカウントがユーザーに代わって EC2 などの関連サービスを呼び出すことを許可する IAM ポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEBSCSIDriverPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 4 月 4 日 17:24 UTC
- 編集日時: 2022 年 11 月 18 日 14:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEC2ContainerRegistryFullAccess

`AmazonEC2ContainerRegistryFullAccess` は、Amazon ECR リソースへの管理アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEC2ContainerRegistryFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 12 月 21 日 17:06 UTC
- 編集日時: 2020 年 12 月 5 日 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
```

```
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEC2ContainerRegistryPowerUser

`AmazonEC2ContainerRegistryPowerUser` は、Amazon EC2 Container Registry リポジトリへのフルアクセスを提供する AWS マネージドポリシーです。ただし、リポジトリの削除やポリシーの変更はできません。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEC2ContainerRegistryPowerUser` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 12 月 21 日 17:05 UTC
- 編集日時: 2019 年 12 月 10 日 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEC2ContainerRegistryReadOnly

AmazonEC2ContainerRegistryReadOnly は、Amazon EC2 Container Registry への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ContainerRegistryReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 12 月 21 日 17:04 UTC
- 編集日時: 2019 年 12 月 10 日 20:56 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEC2ContainerServiceAutoscaleRole

AmazonEC2ContainerServiceAutoscaleRole は、Amazon EC2 Container Service のタスク自動スケーリングを有効にする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ContainerServiceAutoscaleRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 5 月 12 日 23:25 UTC
- 編集日時: 2018 年 2 月 5 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEC2ContainerServiceEventsRole

AmazonEC2ContainerServiceEventsRole は、EC2 Container Service の CloudWatch Events を有効にする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ContainerServiceEventsRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 5 月 30 日 16:51 UTC
- 編集日時: 2023 年 3 月 6 日 22:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEC2ContainerServiceforEC2Role

AmazonEC2ContainerServiceforEC2Role は、Amazon EC2 Container Service の Amazon EC2 ロールのデフォルトポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ContainerServiceforEC2Role をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 3 月 19 日 18:45 UTC
- 編集日時: 2023 年 3 月 6 日 22:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEC2ContainerServiceRole

`AmazonEC2ContainerServiceRole` は、Amazon ECS サービスロールのデフォルトポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ContainerServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 4 月 9 日 16:14 UTC
- 編集日時: 2016 年 8 月 11 日 13:08 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEC2FullAccess

`AmazonEC2FullAccess` は、AWS Management Console 経由で Amazon EC2 へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEC2FullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2018 年 11 月 27 日 02:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEC2ReadOnlyAccess

AmazonEC2ReadOnlyAccess は、経由で Amazon EC2 への読み取り専用アクセスを提供する AWS マネージドポリシーです AWS Management Console。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時： 2024 年 2 月 14 日 18:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonEC2RoleforAWSCodeDeploy

AmazonEC2RoleforAWSCodeDeploy は、リビジョンをダウンロードするための S3 バケットへの EC2 アクセスを許可する AWS マネージドポリシーです。す。EC2 インスタンスの CodeDeploy エージェントには、このロールが必要です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2RoleforAWSCodeDeploy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 5 月 19 日 18:10 UTC
- 編集日時: 2017 年 3 月 20 日 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEC2RoleforAWSCodeDeployLimited

AmazonEC2RoleforAWSCodeDeployLimitedは、リビジョンをダウンロードするための S3 バケットへの制限付きアクセスを EC2 に許可する AWS マネージドポリシーです。EC2 インスタンスの CodeDeploy エージェントには、このロールが必要です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2RoleforAWSCodeDeployLimited をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 8 月 24 日 17:55 UTC
- 編集日時: 2022 年 1 月 20 日 21:37 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEC2RoleforDataPipelineRole

AmazonEC2RoleforDataPipelineRole は、Data Pipeline サービスロールの Amazon EC2 ロールのデフォルトポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2RoleforDataPipelineRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2016 年 2 月 22 日 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEC2RoleforSSM

AmazonEC2RoleforSSM は、まもなく廃止される予定の AWS マネージドポリシーです。AmazonSSMManagedInstanceCore ポリシーを使用して、EC2 インスタンスで AWS Systems Manager サービスコア機能を有効にしてください。詳細は、「https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html」を参照してください。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2RoleforSSM をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 5 月 29 日 17:48 UTC
- 編集日時: 2019 年 1 月 24 日 19:20 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEC2RolePolicyForLaunchWizard

AmazonEC2RolePolicyForLaunchWizard は、EC2 の Amazon LaunchWizard サービスロールのマネージドポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2RolePolicyForLaunchWizard をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 11 月 13 日 08:05 UTC
- 編集日時: 2022 年 5 月 16 日 21:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
        }
      }
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEC2SpotFleetAutoscaleRole

AmazonEC2SpotFleetAutoscaleRole は、Amazon EC2 スポットフリートの自動スケーリングを有効にする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2SpotFleetAutoscaleRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 8 月 19 日 18:27 UTC
- 編集日時: 2019 年 2 月 18 日 19:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEC2SpotFleetTaggingRole

AmazonEC2SpotFleetTaggingRole は、EC2 スポットフリートがお客様に代わってスポットインスタンスをリクエスト、終了、タグ付けできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2SpotFleetTaggingRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 6 月 29 日 18:19 UTC
- 編集日時: 2020 年 4 月 23 日 19:30 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*:*:*/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonECS_FullAccess

AmazonECS_FullAccess は、Amazon ECS リソースへの管理アクセスを提供し、VPC、Auto Scaling グループ、および CloudFormation スタックを含む他の AWS サービスリソースへのアクセスを通じた ECS 機能を有効にする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonECS_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 7 日 21:36 UTC
- 編集日時: 2023 年 1 月 4 日 16:26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonECS_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v20 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
```

```
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerS

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity は、 プライベート認証機関、AWSSecrets Manager、およびユーザーに代わって ECS Service Connect TLS 機能を管理するAWS のサービスために必要なその他の への管理アクセスを提供する AWSマネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成時刻: 2024 年 1 月 19 日 20:08 UTC
- 編集日時： 2024 年 1 月 19 日 20:08 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonECSInfrastructureRolePolicyForVolumes

AmazonECSInfrastructureRolePolicyForVolumes は、ユーザーに代わって ECS ワークロードに関連付けられたボリュームを管理するために必要な他の AWSサービスリソースへのアクセスを提供する AWSマネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonECSInfrastructureRolePolicyForVolumes をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成時刻: 2024 年 1 月 10 日 22:56 UTC
- 編集日時： 2024 年 1 月 10 日 22:56 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonECSServiceRolePolicy

AmazonECSServiceRolePolicy は、Amazon ECS がクラスターを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 14 日 01:18 UTC
- 編集時間:2023 年 12 月 4 日 19:32 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonECSTaskExecutionRolePolicy

AmazonECSTaskExecutionRolePolicy は、Amazon ECS タスクの実行に必要な他の AWS サービスリソースへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonECSTaskExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 11 月 16 日 18:48 UTC
- 編集日時: 2017 年 11 月 16 日 18:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEFSCSIDriverPolicy

AmazonEFSCSIDriverPolicy は、EFS リソースへの管理アクセスと EC2 への読み取りアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEFSCSIDriverPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 7 月 25 日 20:10 UTC
- 編集日時: 2023 年 7 月 25 日 20:10 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEKS_CNI_Policy

AmazonEKS_CNI_Policy は、EKS ワーカーノードの IP アドレス設定を変更するために必要なアクセス許可を Amazon VPC CNI プラグイン (amazon-vpc-cni-k8s) に提供する AWS マネージドポリシーです。このアクセス許可セットにより、CNI はユーザーに代わって Elastic Network Interface の一覧表示、説明、変更を行うことができます。 AWS VPC CNI プラグインの詳細については、https://github.com/aws/amazon-vpc-cni-k8s を参照してください。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKS_CNI_Policy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2018 年 5 月 27 日 21:07 UTC
- 編集日時： 2024 年 3 月 4 日 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonEKSClusterPolicy

AmazonEKSClusterPolicy は、ユーザーに代わってリソースを管理するために必要なアクセス許可を Kubernetes に提供する AWS マネージドポリシーです。Kubernetes では、インスタンス、セキュリティグループ、Elastic Network Interface を含むがこれらに限定されない EC2 リソースに識別情報を配置するには、Ec2:CreateTags 権限が必要です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSClusterPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 5 月 27 日 21:06 UTC
- 編集日時: 2023 年 2 月 7 日 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSClusterPolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEKSConnectorServiceRolePolicy

`AmazonEKSConnectorServiceRolePolicy` は、Amazon EKS が EKS コネクタの AWS リソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 9 月 4 日 20:31 UTC
- 編集日時: 2021 年 9 月 4 日 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSConnectorServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEKSFargatePodExecutionRolePolicy

AmazonEKSFargatePodExecutionRolePolicy は、AWS Fargate で Amazon EKS ポッドを実行するために必要な他の AWS サービスリソースへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSFargatePodExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 11 月 22 日 04:34 UTC
- 編集日時: 2019 年 11 月 22 日 04:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEKSForFargateServiceRolePolicy

`AmazonEKSForFargateServiceRolePolicy` は、Fargate タスクを実行するために必要なアクセス許可を Amazon EKS に付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 22 日 04:36 UTC
- 編集日時: 2019 年 11 月 22 日 04:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSForFargateServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEKSLocalOutpostClusterPolicy

AmazonEKSLocalOutpostClusterPolicy は、アカウントで実行されている EKS ローカルクラスターのコントロールプレーンインスタンスに、ユーザーに代わってリソースを管理するアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSLocalOutpostClusterPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 8 月 24 日 21:56 UTC
- 編集日時: 2022 年 10 月 17 日 16:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*:*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEKSLocalOutpostServiceRolePolicy

`AmazonEKSLocalOutpostServiceRolePolicy` は、Amazon EKS Local がユーザーに代わって AWS サービスを呼び出しできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 8 月 23 日 21:53 UTC
- 編集日時: 2022 年 10 月 24 日 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEKSServicePolicy

AmazonEKSServicePolicy は、Amazon Elastic Container Service for Kubernetes が EKS クラスターを操作するために必要なリソースを作成および管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSServicePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 5 月 27 日 21:08 UTC
- 編集日時: 2020 年 5 月 27 日 19:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSServicePolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEKSServiceRolePolicy

AmazonEKSServiceRolePolicy は、Amazon EKS がユーザーに代わって AWS サービスを呼び出すために必要なサービスリンクロールである AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 2 月 21 日 20:10 UTC
- 編集日時: 2020 年 5 月 27 日 19:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*:*:*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEKSVPCResourceController

`AmazonEKSVPCResourceController` は、VPC リソースコントローラーがワーカーノードの ENI と IP を管理するために使用するポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEKSVPCResourceController` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 8 月 12 日 00:55 UTC
- 編集日時: 2020 年 8 月 12 日 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSVPCResourceController`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEKSWorkerNodePolicy

AmazonEKSWorkerNodePolicy は、Amazon EKS ワーカーノードを Amazon EKS クラスターに接続することを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSWorkerNodePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 5 月 27 日 21:09 UTC
- 編集時間:2023 年 11 月 27 日 00:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElastiCacheFullAccess

`AmazonElastiCacheFullAccess`は、AWS次のような管理ポリシーです。 ElastiCache 経由で Amazon へのフルアクセスを提供しますAWS Management Console。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElastiCacheFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集時間:2023 年 11 月 28 日 03:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElastiCacheReadOnlyAccess

`AmazonElastiCacheReadOnlyAccess` は、AWS Management Console 経由で Amazon ElastiCache への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElastiCacheReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC

- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticContainerRegistryPublicFullAccess

`AmazonElasticContainerRegistryPublicFullAccess` は、Amazon ECR Public リソースへの管理アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticContainerRegistryPublicFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 1 日 17:25 UTC
- 編集日時: 2020 年 12 月 1 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticContainerRegistryPublicPowerUser

AmazonElasticContainerRegistryPublicPowerUser は、Amazon ECR Public リポジトリへのフルアクセスを提供する AWS マネージドポリシーです。ただし、リポジトリの削除やポリシーの変更は許可されません。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticContainerRegistryPublicPowerUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 1 日 16:16 UTC
- 編集日時: 2020 年 12 月 1 日 16:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticContainerRegistryPublicReadOnly

`AmazonElasticContainerRegistryPublicReadOnly` は、Amazon ECR Public リポジトリへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticContainerRegistryPublicReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 1 日 17:27 UTC
- 編集日時: 2020 年 12 月 1 日 17:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticFileSystemClientFullAccess

AmazonElasticFileSystemClientFullAccess は、Amazon EFS ファイルシステムへのルートクライアントアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticFileSystemClientFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 1 月 13 日 16:27 UTC
- 編集日時: 2020 年 1 月 13 日 16:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticFileSystemClientReadOnlyAccess

`AmazonElasticFileSystemClientReadOnlyAccess` は、Amazon EFS ファイルシステムへの読み取り専用のクライアントアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticFileSystemClientReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 1 月 13 日 16:24 UTC

- 編集日時: 2020 年 1 月 13 日 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticFileSystemClientReadWriteAccess

`AmazonElasticFileSystemClientReadWriteAccess` は、Amazon EFS ファイルシステムへの読み取りと書き込みのクライアントアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticFileSystemClientReadWriteAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 1 月 13 日 16:21 UTC
- 編集日時: 2020 年 1 月 13 日 16:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticFileSystemFullAccess

AmazonElasticFileSystemFullAccess は、AWS Management Console経由で Amazon EFS へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticFileSystemFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 5 月 27 日 16:22 UTC
- 編集時間:2023 年 11 月 28 日 16:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticFileSystemReadOnlyAccess

`AmazonElasticFileSystemReadOnlyAccess` は、AWS Management Console 経由で Amazon EFS への読み取り専用アクセスを付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticFileSystemReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 5 月 27 日 16:25 UTC
- 編集日時: 2022 年 1 月 10 日 18:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticFileSystemServiceRolePolicy

`AmazonElasticFileSystemServiceRolePolicy` は、Amazon Elastic File System がユーザーに代わって AWS リソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 5 日 16:52 UTC
- 編集日時: 2022 年 1 月 10 日 19:27 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticFileSystemsUtils

`AmazonElasticFileSystemsUtils` は、AWS Systems Manager を使用して EC2 インスタンスの Amazon EFS ユーティリティ (amazon-efs-utils) パッケージを自動的に管理し、CloudWatchLog を使用して EFS ファイルシステムのマウント成功/失敗の通知を受け取れるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticFileSystemsUtils` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 9 月 29 日 15:16 UTC
- 編集日時: 2020 年 9 月 29 日 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticMapReduceEditorsRole

AmazonElasticMapReduceEditorsRole は、Amazon Elastic MapReduce エディターサービスロールのデフォルトポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticMapReduceEditorsRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 11 月 16 日 21:55 UTC
- 編集日時: 2023 年 2 月 9 日 22:39 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticMapReduceforAutoScalingRole

AmazonElasticMapReduceforAutoScalingRole は、Auto Scaling 用の Amazon Elastic MapReduce である AWS マネージドポリシーです。Auto Scaling が EMR クラスターにインスタンスを追加および削除できるようにするロールです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticMapReduceforAutoScalingRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 11 月 18 日 01:09 UTC
- 編集日時: 2016 年 11 月 18 日 01:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticMapReduceforEC2Role

`AmazonElasticMapReduceforEC2Role` は、Amazon Elastic MapReduce for EC2 サービスロールのデフォルトポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticMapReduceforEC2Role` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2017 年 8 月 11 日 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticMapReduceFullAccess

`AmazonElasticMapReduceFullAccess` は、廃止予定の AWS マネージドポリシーです。ガイダンスについては、「https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html」のドキュメントを参照してください。Amazon Elastic MapReduce とそれが必要とする基盤となるサービス (EC2 や S3 など) へのフルアクセスを提供します

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticMapReduceFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2019 年 10 月 11 日 15:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
```

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticMapReducePlacementGroupPolicy

`AmazonElasticMapReducePlacementGroupPolicy` は、EMR が EC2 プレイスメントグループを作成、記述、削除できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticMapReducePlacementGroupPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 9 月 29 日 00:37 UTC
- 編集日時: 2020 年 9 月 29 日 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticMapReduceReadOnlyAccess

`AmazonElasticMapReduceReadOnlyAccess` は、AWS Management Console 経由で Amazon Elastic MapReduce への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticMapReduceReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2020 年 7 月 29 日 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticMapReduceRole

AmazonElasticMapReduceRole は、廃止予定の AWS マネージドポリシーです。ガイダンスについては、「https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html」のドキュメントを参照してください。Amazon Elastic MapReduce サービスロールのデフォルトポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticMapReduceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2020 年 6 月 24 日 22:24 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticsearchServiceRolePolicy

`AmazonElasticsearchServiceRolePolicy` は、Amazon Elasticsearch Service がユーザーに代わって EC2 ネットワーク API などの他の AWS サービスにアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 7 月 7 日 00:15 UTC
- 編集日時: 2023 年 10 月 23 日 06:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticTranscoder_FullAccess

AmazonElasticTranscoder_FullAccess は、Elastic Transcoder へのフルアクセスと、Elastic Transcoder の全機能に必要な関連サービスへのアクセスをユーザーに付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticTranscoder_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 4 月 27 日 18:59 UTC
- 編集日時: 2019 年 6 月 10 日 22:51 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticTranscoder_JobsSubmitter

`AmazonElasticTranscoder_JobsSubmitter` は、プリセットの変更、ジョブの送信、Elastic Transcoder 設定の表示を行うアクセス許可をユーザーに付与する AWS マネージドポリシーです。このポリシーでは、S3、IAM、SNS など、Elastic Transcode コンソールの使用に必要なその他のサービスへの読み取り専用アクセスも一部付与されます。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticTranscoder_JobsSubmitter` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 6 月 7 日 21:12 UTC
- 編集日時: 2019 年 6 月 10 日 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticTranscoder_ReadOnlyAccess

AmazonElasticTranscoder_ReadOnlyAccess は、Elastic Transcoder への読み取り専用のアクセスと、関連サービスへのリストアクセスをユーザーに付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticTranscoder_ReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 6 月 7 日 21:09 UTC
- 編集日時: 2019 年 6 月 10 日 22:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonElasticTranscoderRole

`AmazonElasticTranscoderRole` は、Amazon Elastic Transcoder サービスロールのデフォルトポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonElasticTranscoderRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2019 年 6 月 13 日 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEMRCleanupPolicy

AmazonEMRCleanupPolicy は、EMR サービスロールが AWS EC2 リソースの終了と削除を実行できなくなった場合に、EMR が必要とするアクションを可能にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 26 日 23:54 UTC
- 編集日時: 2020 年 9 月 29 日 21:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEMRContainersServiceRolePolicy

`AmazonEMRContainersServiceRolePolicy` は、Amazon EMR の実行に必要な他の AWS サービスリソースにアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 9 日 00:38 UTC

- 編集日時: 2023 年 3 月 10 日 22:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEMRFullAccessPolicy_v2

AmazonEMRFullAccessPolicy_v2 は、Amazon EMR へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEMRFullAccessPolicy_v2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 3 月 12 日 01:50 UTC
- 編集日時: 2023 年 7 月 28 日 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEMRReadOnlyAccessPolicy_v2

AmazonEMRReadOnlyAccessPolicy_v2 は、Amazon EMR および関連する CloudWatch メトリックスへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEMRReadOnlyAccessPolicy_v2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 3 月 12 日 01:39 UTC
- 編集日時: 2023 年 8 月 2 日 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEMRServerlessServiceRolePolicy

`AmazonEMRServerlessServiceRolePolicy` は、Amazon EMRServerless の実行に必要な他の AWS サービスリソースにアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 5 月 20 日 23:15 UTC

- 編集日時： 2024 年 1 月 25 日 18:21 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEMRServicePolicy_v2

AmazonEMRServicePolicy_v2 は、Amazon EMR サービスロールに使用される AWS マネージドポリシーです、アカウントの他の IAM ユーザーやロールには使用しないでください。このポリシーは、EMR クラスターのオペレーションに必要な EMR および関連サービスに関連するリソースを作成および管理するためのアクセス許可を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEMRServicePolicy_v2 をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 3 月 12 日 01:11 UTC
- 編集日時: 2022 年 2 月 15 日 16:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonESCognitoAccess

`AmazonESCognitoAccess` は、Amazon Cognito 設定サービスへの制限付きアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonESCognitoAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 2 月 28 日 22:29 UTC
- 編集日時: 2021 年 12 月 20 日 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonESCognitoAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonESFullAccess

`AmazonESFullAccess` は、Amazon ES 設定サービスへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonESFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 10 月 1 日 19:14 UTC

- 編集日時: 2015 年 10 月 1 日 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonESReadOnlyAccess

`AmazonESReadOnlyAccess` は、Amazon ES 設定サービスへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonESReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 10 月 1 日 19:18 UTC
- 編集日時: 2018 年 10 月 3 日 03:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonESReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEventBridgeApiDestinationsServiceRolePolicy

AmazonEventBridgeApiDestinationsServiceRolePolicy は、EventBridge がユーザーに代わってシークレットマネージャーのリソースにアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 2 月 11 日 20:52 UTC
- 編集日時: 2021 年 2 月 11 日 20:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "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/*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEventBridgeFullAccess

`AmazonEventBridgeFullAccess` は、Amazon EventBridge へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEventBridgeFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 7 月 11 日 14:08 UTC
- 編集日時: 2022 年 12 月 1 日 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEventBridgePipesFullAccess

`AmazonEventBridgePipesFullAccess` は、Amazon EventBridge Pipes へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEventBridgePipesFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 12 月 1 日 17:03 UTC
- 編集日時: 2022 年 12 月 1 日 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEventBridgePipesOperatorAccess

AmazonEventBridgePipesOperatorAccess は、Amazon EventBridge Pipes への読み取り専用アクセスとオペレーターアクセス (つまり、Pipes の実行を停止および開始する機能) を提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEventBridgePipesOperatorAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 12 月 1 日 17:04 UTC
- 編集日時: 2022 年 12 月 1 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEventBridgePipesReadOnlyAccess

`AmazonEventBridgePipesReadOnlyAccess` は、Amazon EventBridge Pipes への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEventBridgePipesReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 12 月 1 日 17:04 UTC
- 編集日時: 2022 年 12 月 1 日 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEventBridgeReadOnlyAccess

AmazonEventBridgeReadOnlyAccess は、Amazon EventBridge への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEventBridgeReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 7 月 11 日 13:59 UTC

- 編集日時: 2022 年 12 月 1 日 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEventBridgeSchedulerFullAccess

`AmazonEventBridgeSchedulerFullAccess` は、AmazonEventBridgeSchedulerFullAccess マネージドポリシーであり、スケジュールおよびスケジュールグループに対してすべての EventBridge スケジューラアクションを使用するアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEventBridgeSchedulerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 10 日 18:37 UTC
- 編集日時: 2022 年 11 月 10 日 18:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
```

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEventBridgeSchedulerReadOnlyAccess

`AmazonEventBridgeSchedulerReadOnlyAccess` は、AmazonEventBridgeSchedulerReadOnlyAccess マネージドポリシーであり、お客様のスケジュールとスケジュールグループに関する詳細を表示する読み取り専用アクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEventBridgeSchedulerReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 10 日 18:50 UTC
- 編集日時: 2022 年 11 月 10 日 18:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEventBridgeSchemasFullAccess

`AmazonEventBridgeSchemasFullAccess` は、Amazon EventBridge スキーマへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEventBridgeSchemasFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2019 年 11 月 28 日 23:12 UTC
- 編集日時: 2019 年 11 月 28 日 23:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEventBridgeSchemasReadOnlyAccess

AmazonEventBridgeSchemasReadOnlyAccess は、Amazon EventBridge スキーマへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEventBridgeSchemasReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 11 月 28 日 23:05 UTC
- 編集日時: 2020 年 5 月 1 日 00:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonEventBridgeSchemasServiceRolePolicy

AmazonEventBridgeSchemasServiceRolePolicy は、Amazon EventBridge スキーマによって作成されたマネージドルールにアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 27 日 01:10 UTC
- 編集日時: 2019 年 11 月 27 日 01:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonFISServiceRolePolicy

AmazonFISServiceRolePolicy は、AWS FIS が実験のモニタリングとリソース選択をできるようにするためのポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 21 日 21:18 UTC
- 編集日時: 2022 年 10 月 25 日 09:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonForecastFullAccess

AmazonForecastFullAccess は、Amazon Forecast のすべてのアクションへのアクセスを許可する AWS マネージドポリシーです

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonForecastFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 1 月 18 日 01:52 UTC
- 編集日時: 2019 年 1 月 18 日 01:52 UTC
- ARN: arn:aws:iam::aws:policy/AmazonForecastFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "forecast:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonFraudDetectorFullAccessPolicy

`AmazonFraudDetectorFullAccessPolicy` は、Amazon Fraud Detector のすべてのアクションへのアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonFraudDetectorFullAccessPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 3 日 22:46 UTC
- 編集日時: 2019 年 12 月 3 日 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonFreeRTOSFullAccess

`AmazonFreeRTOSFullAccess` は、Amazon FreeRTOS のフルアクセスポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonFreeRTOSFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 29 日 15:32 UTC
- 編集日時: 2017 年 11 月 29 日 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonFreeRTOSOTAUpdate

`AmazonFreeRTOSOTAUpdate` は、ユーザーが Amazon FreeRTOS OTA アップデートにアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonFreeRTOSOTAUpdate` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 8 月 27 日 22:43 UTC
- 編集日時: 2020 年 12 月 18 日 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonFSxConsoleFullAccess

`AmazonFSxConsoleFullAccess` は、Amazon FSx へのフルアクセスおよび AWS Management Console経由での AWS に関連するサービスへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonFSxConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 28 日 16:36 UTC
- 編集日時： 2024 年 1 月 10 日 20:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonFSxConsoleReadOnlyAccess

AmazonFSxConsoleReadOnlyAccess は、Amazon FSx への読み取り専用アクセス許可および AWS Management Console経由での AWS に関連するサービスへのアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonFSxConsoleReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 28 日 16:35 UTC
- 編集日時： 2024 年 1 月 10 日 20:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonFSxFullAccess

AmazonFSxFullAccess は、Amazon FSx へのフルアクセスと、関連する AWS サービスへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonFSxFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 28 日 16:34 UTC

- 編集日時： 2024 年 1 月 10 日 20:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxFullAccess

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonFSxReadOnlyAccess

`AmazonFSxReadOnlyAccess` は、Amazon FSx への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonFSxReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 28 日 16:33 UTC
- 編集日時: 2018 年 11 月 28 日 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonFSxServiceRolePolicy

`AmazonFSxServiceRolePolicy` は、Amazon FSx がユーザーに代わって AWS リソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 28 日 10:38 UTC
- 編集日時： 2024 年 1 月 10 日 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonGlacierFullAccess

`AmazonGlacierFullAccess` は、AWS Management Console 経由で Amazon Glacier へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonGlacierFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonGlacierReadOnlyAccess

`AmazonGlacierReadOnlyAccess` は、AWS Management Console 経由で Amazon Glacier への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonGlacierReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2016 年 5 月 5 日 18:46 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonGrafanaAthenaAccess

AmazonGrafanaAthenaAccess は、Amazon Athena と、Amazon Grafana の Amazon Athena プラグインからクエリを実行して S3 に結果を書き込むために必要な依存関係へのアクセス権を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonGrafanaAthenaAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 22 日 17:11 UTC
- 編集日時: 2021 年 11 月 22 日 17:11 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonGrafanaCloudWatchAccess

`AmazonGrafanaCloudWatchAccess` は、Amazon CloudWatch と、CloudWatch を Amazon Managed Grafana 内のデータソースとして使用するために必要な依存関係へのアクセス権を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonGrafanaCloudWatchAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2023 年 3 月 24 日 22:41 UTC
- 編集日時: 2023 年 3 月 24 日 22:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonGrafanaRedshiftAccess

`AmazonGrafanaRedshiftAccess` は、Amazon Redshift と、Amazon Grafana で Amazon Redshift プラグインを使用するために必要な依存関係へのスコープ付きアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonGrafanaRedshiftAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 26 日 23:15 UTC
- 編集日時: 2021 年 11 月 26 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonGrafanaServiceLinkedRolePolicy

AmazonGrafanaServiceLinkedRolePolicy は、Amazon Grafana が管理または使用する AWS リソースへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 8 日 23:10 UTC
- 編集日時: 2022 年 11 月 8 日 23:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonGuardDutyFullAccess

AmazonGuardDutyFullAccessは、Amazon AWSを使用するためのフルアクセスを提供する管理ポリシーです GuardDuty。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonGuardDutyFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 28 日 22:31 UTC
- 編集時間:2023 年 11 月 16 日 23:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonGuardDutyMalwareProtectionServiceRolePolicy

`AmazonGuardDutyMalwareProtectionServiceRolePolicy` は、 GuardDuty マルウェア保護が という名前のサービスにリンクされたロール (SLR) を使用する AWSマネージドポリシーです AWSServiceRoleForAmazonGuardDutyMalwareProtection。このサービスにリンクされたロールにより、 GuardDuty マルウェア保護はエージェントレススキャンを実行してマルウェアを検出できます。これにより、 GuardDuty はアカウントでスナップショットを作成し、 GuardDuty サービスアカウントとスナップショットを共有してマルウェアをスキャンできます。これらの共有スナップショットを評価し、取得した EC2 インスタンスメタデータを GuardDuty Malware Protection の検出結果に含めます。 AWSServiceRoleForAmazonGuardDutyMalwareProtection サービスにリンクされたロールは、malware-protection.guardduty.amazonaws.com サービスを信頼してロールを引き受けます。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 7 月 19 日 19:06 UTC
- 編集日時： 2024 年 1 月 25 日 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonGuardDutyReadOnlyAccess

AmazonGuardDutyReadOnlyAccessは、Amazon AWS GuardDuty リソースへの読み取り専用アクセスを提供する管理ポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonGuardDutyReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2017 年 11 月 28 日 22:29 UTC
- 編集時間:2023 年 11 月 16 日 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonGuardDutyServiceRolePolicy

AmazonGuardDutyServiceRolePolicy は、Amazon Guard Duty が使用または管理する AWS リソースへのアクセスを有効にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 28 日 20:12 UTC
- 編集日時： 2024 年 2 月 9 日 18:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonHealthLakeFullAccess

AmazonHealthLakeFullAccess は、Amazon HealthLake サービスへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHealthLakeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 2 月 17 日 01:07 UTC
- 編集日時: 2021 年 2 月 17 日 01:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonHealthLakeReadOnlyAccess

`AmazonHealthLakeReadOnlyAccess` は、Amazon HealthLake サービスへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonHealthLakeReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 2 月 17 日 02:43 UTC
- 編集日時: 2021 年 2 月 17 日 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonHoneycodeFullAccess

AmazonHoneycodeFullAccess は、AWS Management Console および SDK 経由で Honeycode へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHoneycodeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 6 月 24 日 20:28 UTC
- 編集日時: 2020 年 6 月 24 日 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonHoneycodeReadOnlyAccess

AmazonHoneycodeReadOnlyAccess は、AWS Management Console および SDK 経由で Honeycode への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHoneycodeReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 6 月 24 日 20:28 UTC
- 編集日時: 2020 年 12 月 1 日 17:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonHoneycodeServiceRolePolicy

AmazonHoneycodeServiceRolePolicy は、Amazon Honeycode がリソースにアクセスする際に必要となる、サービスリンクロールである AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 18 日 18:03 UTC
- 編集日時: 2020 年 11 月 18 日 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonHoneycodeTeamAssociationFullAccess

AmazonHoneycodeTeamAssociationFullAccess は、AWS Management Console および SDK 経由で Honeycode Team Association へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHoneycodeTeamAssociationFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 6 月 24 日 20:28 UTC
- 編集日時: 2020 年 6 月 24 日 20:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonHoneycodeTeamAssociationReadOnlyAccess

`AmazonHoneycodeTeamAssociationReadOnlyAccess` は、AWS Management Console および SDK 経由で Honeycode Team Association への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHoneycodeTeamAssociationReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 6 月 24 日 20:27 UTC
- 編集日時: 2020 年 6 月 24 日 20:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonHoneycodeWorkbookFullAccess

AmazonHoneycodeWorkbookFullAccess は、AWS Management Console および SDK 経由で Honeycode Workbook へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHoneycodeWorkbookFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 6 月 24 日 20:28 UTC
- 編集日時: 2020 年 12 月 1 日 17:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonHoneycodeWorkbookReadOnlyAccess

`AmazonHoneycodeWorkbookReadOnlyAccess` は、AWS Management Console および SDK 経由で Honeycode Workbook への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonHoneycodeWorkbookReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2020 年 6 月 24 日 20:28 UTC
- 編集日時: 2020 年 12 月 1 日 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonInspector2AgentlessServiceRolePolicy

AmazonInspector2AgentlessServiceRolePolicyは、AWS のサービスエージェントレスのセキュリティ評価を実行するために必要なアクセス権限を Amazon Inspector AWSに付与する管理ポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成時間:2023 年 11 月 20 日 15:18 UTC
- 編集時間:2023 年 11 月 20 日 15:18 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonInspector2FullAccess

`AmazonInspector2FullAccess` は、Amazon Inspector へのフルアクセスと、組織などの他の関連サービスへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonInspector2FullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 29 日 19:10 UTC
- 編集日時: 2023 年 8 月 3 日 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonInspector2ManagedCisPolicy

AmazonInspector2ManagedCisPolicy は、CIS スキャンのためにインスペクターサービスと通信するためにお客様がロールにアタッチする必要がある マネージドポリシーですAWS。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonInspector2ManagedCisPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時刻: 2024 年 1 月 24 日 16:31 UTC
- 編集日時： 2024 年 1 月 24 日 16:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonInspector2ReadOnlyAccess

AmazonInspector2ReadOnlyAccess は、Amazon inspector2 サービスと関連するサポートサービスへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonInspector2ReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2022 年 1 月 21 日 14:45 UTC
- 編集日時: 2023 年 9 月 22 日 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonInspector2ServiceRolePolicy

`AmazonInspector2ServiceRolePolicy` は、セキュリティ評価を実行するために必要な AWS のサービス へのアクセス権を Amazon Inspector に付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 16 日 20:27 UTC
- 編集日時： 2024 年 1 月 22 日 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v12 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonInspectorFullAccess

`AmazonInspectorFullAccess` は、Amazon Inspector へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonInspectorFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 10 月 7 日 17:08 UTC
- 編集日時: 2017 年 12 月 21 日 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonInspectorReadOnlyAccess

`AmazonInspectorReadOnlyAccess` は、Amazon Inspector への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonInspectorReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 10 月 7 日 17:08 UTC
- 編集日時: 2019 年 10 月 1 日 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonInspectorServiceRolePolicy

AmazonInspectorServiceRolePolicy は、セキュリティ評価を実行するために必要な AWS のサービス へのアクセス権を Amazon Inspector に付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 21 日 15:48 UTC
- 編集日時: 2020 年 9 月 11 日 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonKendraFullAccess

AmazonKendraFullAccess は、AWS Management Console 経由で Amazon Kendra へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKendraFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 3 日 16:15 UTC
- 編集日時: 2019 年 12 月 3 日 16:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKendraFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonKendraReadOnlyAccess

`AmazonKendraReadOnlyAccess` は、AWS Management Console 経由で Amazon Kendra への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonKendraReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 3 日 16:13 UTC

- 編集日時: 2021 年 5 月 27 日 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonKeyspacesFullAccess

AmazonKeyspacesFullAccess は、Amazon Keyspaces へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKeyspacesFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 4 月 23 日 17:06 UTC
- 編集日時: 2023 年 10 月 3 日 19:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonKeyspacesReadOnlyAccess

`AmazonKeyspacesReadOnlyAccess` は、Amazon Keyspaces への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonKeyspacesReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2020 年 4 月 23 日 17:07 UTC
- 編集日時: 2022 年 7 月 7 日 14:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonKeyspacesReadOnlyAccess_v2

AmazonKeyspacesReadOnlyAccess_v2 は、Amazon Keyspaces および AWS 関連サービスへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKeyspacesReadOnlyAccess_v2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 9 月 12 日 17:01 UTC
- 編集日時: 2023 年 9 月 12 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonKinesisAnalyticsFullAccess

AmazonKinesisAnalyticsFullAccess は、AWS Management Console 経由で Amazon Kinesis Analytics へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKinesisAnalyticsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 9 月 21 日 19:01 UTC
- 編集日時: 2016 年 9 月 21 日 19:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonKinesisAnalyticsReadOnly

`AmazonKinesisAnalyticsReadOnly` は、AWS Management Console 経由で Amazon Kinesis Analytics への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonKinesisAnalyticsReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 9 月 21 日 18:16 UTC
- 編集日時: 2016 年 9 月 21 日 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
```

```
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonKinesisFirehoseFullAccess

`AmazonKinesisFirehoseFullAccess` は、すべての Amazon Kinesis Firehose デリバリーストリームへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonKinesisFirehoseFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 10 月 7 日 18:45 UTC
- 編集日時: 2015 年 10 月 7 日 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonKinesisFirehoseReadOnlyAccess

`AmazonKinesisFirehoseReadOnlyAccess` は、すべての Amazon Kinesis Firehose デリバリーストリームへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonKinesisFirehoseReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 10 月 7 日 18:43 UTC
- 編集日時: 2015 年 10 月 7 日 18:43 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonKinesisFullAccess

`AmazonKinesisFullAccess` は、AWS Management Console 経由ですべてのストリームへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKinesisFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonKinesisReadOnlyAccess

AmazonKinesisReadOnlyAccess は、AWS Management Console 経由のすべてのストリームへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKinesisReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonKinesisVideoStreamsFullAccess

`AmazonKinesisVideoStreamsFullAccess` は、AWS Management Console 経由で Amazon Kinesis Video Streams へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonKinesisVideoStreamsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 12 月 1 日 23:27 UTC
- 編集日時: 2017 年 12 月 1 日 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonKinesisVideoStreamsReadOnlyAccess

`AmazonKinesisVideoStreamsReadOnlyAccess` は、AWS Management Console 経由で AWS Kinesis Video Streams への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonKinesisVideoStreamsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 12 月 1 日 23:14 UTC
- 編集日時: 2017 年 12 月 1 日 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonLaunchWizard_Fullaccess

AmazonLaunchWizard_Fullaccess は、AWS 起動ウィザードやその他の必要なサービスへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLaunchWizard_Fullaccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 8 月 6 日 17:47 UTC
- 編集日時: 2023 年 2 月 22 日 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess`

ポリシーのバージョン

ポリシーのバージョン: v15 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonLaunchWizardFullAccessV2

AmazonLaunchWizardFullAccessV2 は、AWS 起動ウィザードやその他の必要なサービスへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLaunchWizardFullAccessV2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 9 月 1 日 17:14 UTC
- 編集日時: 2023 年 9 月 1 日 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonLexChannelsAccess

AmazonLexChannelsAccess は、お客様がチャネルから Lex ランタイムを呼び出すことができるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 1 月 13 日 20:12 UTC
- 編集日時: 2021 年 1 月 13 日 20:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonLexFullAccess

AmazonLexFullAccess は、経由で Amazon Lex へのフルアクセスを提供する AWS マネージドポリシーです AWS Management Console。また、Lex サービスにリンクされたロールを作成し、限定された Lambda 関数セットを呼び出すための Lex アクセス許可を付与するためのアクセスも提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLexFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 4 月 11 日 23:20 UTC
- 編集日時： 2024 年 2 月 7 日 00:55 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLexFullAccess

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonLexReadOnly

AmazonLexReadOnly は、Amazon Lex への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLexReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 4 月 11 日 23:13 UTC

- 編集日時: 2023 年 1 月 31 日 19:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonLexReplicationPolicy

`AmazonLexReplicationPolicy` は、Amazon Lex がユーザーに代わってリージョン間で Lex リソースをレプリケートできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成時刻: 2024 年 1 月 31 日 23:29 UTC
- 編集日時： 2024 年 3 月 8 日 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonLexRunBotsOnly

AmazonLexRunBotsOnly は、Amazon Lex の会話型 API へのアクセスを提供する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLexRunBotsOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 4 月 11 日 23:06 UTC
- 編集日時: 2021 年 8 月 18 日 00:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLexRunBotsOnly

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonLexV2BotPolicy

AmazonLexV2BotPolicy は、ユーザーに代わって他の AWS サービスを呼び出すためのアクセスを Lex V2 ボットに提供する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 1 月 13 日 20:10 UTC
- 編集日時: 2021 年 1 月 13 日 20:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonLookoutEquipmentFullAccess

AmazonLookoutEquipmentFullAccess は、Amazon Lookout for Equipment オペレーションへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLookoutEquipmentFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 4 月 8 日 15:52 UTC
- 編集日時: 2021 年 11 月 24 日 21:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonLookoutEquipmentReadOnlyAccess

AmazonLookoutEquipmentReadOnlyAccess は、Amazon Lookout for Equipment への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLookoutEquipmentReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 5 月 5 日 16:47 UTC
- 編集日時: 2022 年 11 月 10 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonLookoutMetricsFullAccess

`AmazonLookoutMetricsFullAccess` は、Amazon Lookout for Metrics のすべてのアクションへのアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonLookoutMetricsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2021 年 5 月 7 日 00:43 UTC
- 編集日時: 2021 年 5 月 7 日 00:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonLookoutMetricsReadOnlyAccess

AmazonLookoutMetricsReadOnlyAccessは、Amazon Lookout for Metrics のすべての読み取り専用アクションへのアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLookoutMetricsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 5 月 7 日 00:43 UTC
- 編集日時: 2022 年 1 月 4 日 18:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonLookoutVisionConsoleFullAccess

`AmazonLookoutVisionConsoleFullAccess` は、Amazon Lookout for Vision へのフルアクセスと、必要なサービスとコンソールの依存関係へのスコープ付きアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLookoutVisionConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 5 月 11 日 19:37 UTC
- 編集日時: 2021 年 5 月 11 日 19:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonLookoutVisionConsoleReadOnlyAccess

AmazonLookoutVisionConsoleReadOnlyAccess は、Amazon Lookout for Vision への読み取り専用アクセスと、必要なサービスとコンソールの依存関係へのスコープ付きアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLookoutVisionConsoleReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 5 月 11 日 19:32 UTC
- 編集日時: 2021 年 12 月 9 日 02:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonLookoutVisionFullAccess

AmazonLookoutVisionFullAccess は、Amazon Lookout for Vision へのフルアクセスと、必要な依存関係へのスコープ付きアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLookoutVisionFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 5 月 11 日 19:24 UTC
- 編集日時: 2021 年 5 月 11 日 19:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:*"
      ],
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonLookoutVisionReadOnlyAccess

AmazonLookoutVisionReadOnlyAccess は、Amazon Lookout for Vision への読み取り専用アクセスと、必要な依存関係へのスコープ付きアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLookoutVisionReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 5 月 11 日 19:11 UTC
- 編集日時: 2021 年 12 月 9 日 03:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMachineLearningBatchPredictionsAccess

AmazonMachineLearningBatchPredictionsAccess は、Amazon Machine Learning のバッチ予測をリクエストするアクセス許可をユーザーに付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMachineLearningBatchPredictionsAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 4 月 9 日 17:12 UTC
- 編集日時: 2015 年 4 月 9 日 17:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning:DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMachineLearningCreateOnlyAccess

`AmazonMachineLearningCreateOnlyAccess` は、予測以外の Amazon Machine Learning リソースの作成アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMachineLearningCreateOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 4 月 9 日 17:18 UTC
- 編集日時: 2016 年 6 月 29 日 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning:Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMachineLearningFullAccess

AmazonMachineLearningFullAccess は、Amazon Machine Learning リソースへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMachineLearningFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 4 月 9 日 17:25 UTC
- 編集日時: 2015 年 4 月 9 日 17:25 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

`AmazonMachineLearningManageRealTimeEndpointOnlyAccess` は、Amazon Machine Learning モデルのリアルタイムエンドポイントを作成および削除するアクセス許可をユーザーに付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMachineLearningManageRealTimeEndpointOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 4 月 9 日 17:32 UTC
- 編集日時: 2015 年 4 月 9 日 17:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMachineLearningReadOnlyAccess

`AmazonMachineLearningReadOnlyAccess` は、Amazon Machine Learning リソースへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMachineLearningReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 4 月 9 日 17:40 UTC
- 編集日時: 2015 年 4 月 9 日 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMachineLearningRealTimePredictionOnlyAccess

`AmazonMachineLearningRealTimePredictionOnlyAccess` は、Amazon Machine Learning のリアルタイム予測をリクエストするアクセス権限をユーザーに付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMachineLearningRealTimePredictionOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 4 月 9 日 17:44 UTC
- 編集日時: 2015 年 4 月 9 日 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMachineLearningRoleforRedshiftDataSourceV3

`AmazonMachineLearningRoleforRedshiftDataSourceV3` は、Machine Learning が Redshift データソースの Redshift クラスターと S3 ステージング場所を設定して使用できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMachineLearningRoleforRedshiftDataSourceV3 をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 24 日 18:00 UTC
- 編集日時: 2020 年 6 月 24 日 18:00 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMacieFullAccess

`AmazonMacieFullAccess` は、Amazon Macie へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMacieFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 8 月 14 日 14:54 UTC
- 編集日時: 2022 年 7 月 1 日 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMacieHandshakeRole

AmazonMacieHandshakeRole は、Amazon Macie のサービスリンクロールを作成するアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMacieHandshakeRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 6 月 28 日 15:46 UTC
- 編集日時: 2018 年 6 月 28 日 15:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMacieReadOnlyAccess

`AmazonMacieReadOnlyAccess` は、Amazon Macie への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMacieReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 6 月 15 日 21:50 UTC
- 編集日時: 2023 年 6 月 15 日 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMacieServiceRole

AmazonMacieServiceRole は、データ分析を可能にするため、アカウント内のリソース依存関係への読み取りのみアクセスを Macie に付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMacieServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 8 月 14 日 14:53 UTC
- 編集日時: 2017 年 8 月 14 日 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMacieServiceRolePolicy

AmazonMacieServiceRolePolicy は、Amazon Macie のサービスリンクロールである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 6 月 19 日 22:17 UTC
- 編集日時: 2022 年 5 月 19 日 19:16 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonManagedBlockchainConsoleFullAccess

AmazonManagedBlockchainConsoleFullAccess は、AWS Management Console 経由で Amazon Managed Blockchain へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonManagedBlockchainConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 4 月 29 日 21:23 UTC
- 編集日時: 2019 年 4 月 29 日 21:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonManagedBlockchainFullAccess

AmazonManagedBlockchainFullAccess は、Amazon Managed Blockchain へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonManagedBlockchainFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 4 月 29 日 21:39 UTC
- 編集日時: 2019 年 4 月 29 日 21:39 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonManagedBlockchainReadOnlyAccess

`AmazonManagedBlockchainReadOnlyAccess` は、Amazon Managed Blockchain への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonManagedBlockchainReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 4 月 30 日 18:17 UTC
- 編集日時: 2019 年 4 月 30 日 18:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonManagedBlockchainServiceRolePolicy

AmazonManagedBlockchainServiceRolePolicy は、Amazon Managed Blockchain が使用または管理する AWS のサービス およびリソースへのアクセスを可能にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 1 月 17 日 19:51 UTC
- 編集日時: 2020 年 1 月 17 日 19:51 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMCSFullAccess

AmazonMCSFullAccess は、Amazon Managed Apache Cassandra サービスへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMCSFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 3 日 13:45 UTC
- 編集日時: 2020 年 4 月 17 日 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMCSReadOnlyAccess

`AmazonMCSReadOnlyAccess` は、Amazon Managed Apache Cassandra サービスへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMCSReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 3 日 13:46 UTC
- 編集日時: 2020 年 4 月 17 日 19:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMechanicalTurkFullAccess

`AmazonMechanicalTurkFullAccess` は、Amazon Mechanical Turk のすべての API へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMechanicalTurkFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 12 月 11 日 19:08 UTC
- 編集日時: 2015 年 12 月 11 日 19:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMechanicalTurkReadOnly

`AmazonMechanicalTurkReadOnly` は、Amazon Mechanical Turk の読み取り専用 API へのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMechanicalTurkReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 12 月 11 日 19:08 UTC

- 編集日時: 2019 年 9 月 25 日 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMemoryDBFullAccess

AmazonMemoryDBFullAccess は、AWS Management Console 経由で Amazon MemoryDB へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMemoryDBFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 10 月 8 日 19:24 UTC
- 編集日時: 2021 年 10 月 8 日 19:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMemoryDBReadOnlyAccess

`AmazonMemoryDBReadOnlyAccess` は、AWS Management Console 経由で Amazon MemoryDB への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMemoryDBReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 10 月 8 日 19:27 UTC
- 編集日時: 2021 年 10 月 8 日 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMobileAnalyticsFinancialReportAccess

AmazonMobileAnalyticsFinancialReportAccess は、すべてのアプリケーションリソースの財務データを含むすべてのレポートへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMobileAnalyticsFinancialReportAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMobileAnalyticsFullAccess

AmazonMobileAnalyticsFullAccess は、すべてのアプリケーションリソースへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMobileAnalyticsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMobileAnalyticsNon-financialReportAccess

AmazonMobileAnalyticsNon-financialReportAccess は、すべてのアプリケーションリソースの非財務レポートへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMobileAnalyticsNon-financialReportAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mobileanalytics:GetReports",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMobileAnalyticsWriteOnlyAccess

AmazonMobileAnalyticsWriteOnlyAccess は、すべてのアプリケーションリソースのイベントデータを格納するための書き込み専用アクセスを提供する AWS マネージドポリシーです。(SDK 統合に推奨)

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMobileAnalyticsWriteOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMonitronFullAccess

`AmazonMonitronFullAccess` は、Amazon Monitron を管理するためのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMonitronFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 2 日 22:40 UTC
- 編集日時: 2022 年 6 月 8 日 16:27 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMQApiFullAccess

`AmazonMQApiFullAccess` は、API/SDK 経由で AmazonMQ へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMQApiFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 12 月 18 日 20:31 UTC
- 編集日時: 2020 年 11 月 4 日 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMQApiReadOnlyAccess

AmazonMQApiReadOnlyAccess は、API/SDK 経由で AmazonMQ への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMQApiReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 12 月 18 日 20:31 UTC
- 編集日時: 2018 年 12 月 18 日 20:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMQFullAccess

`AmazonMQFullAccess` は、AWS Management Console 経由で AmazonMQ へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMQFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 28 日 15:28 UTC
- 編集日時: 2020 年 11 月 4 日 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMQReadOnlyAccess

`AmazonMQReadOnlyAccess` は、AWS Management Console 経由で AmazonMQ への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMQReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 28 日 15:30 UTC
- 編集日時: 2017 年 11 月 28 日 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMQServiceRolePolicy

AmazonMQServiceRolePolicy は、AWS Amazon MQ のサービスリンクロールポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 4 日 16:07 UTC
- 編集日時: 2020 年 11 月 4 日 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMSKConnectReadOnlyAccess

AmazonMSKConnectReadOnlyAccess は、Amazon MSK Connect への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMSKConnectReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 9 月 20 日 10:18 UTC
- 編集日時: 2021 年 10 月 18 日 09:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
```

```
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMSKFullAccess

`AmazonMSKFullAccess` は、Amazon MSK へのフルアクセスと、その依存関係に必要なその他のアクセス許可を提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMSKFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 1 月 14 日 22:07 UTC
- 編集日時: 2023 年 10 月 18 日 11:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMSKReadOnlyAccess

AmazonMSKReadOnlyAccess は、Amazon MSK への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMSKReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 1 月 14 日 22:28 UTC
- 編集日時: 2019 年 1 月 14 日 22:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonMWAAServiceRolePolicy

AmazonMWAAServiceRolePolicy は、Apache Airflow 用の Amazon マネージドワークフローで使用されるサービスリンクロールである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 24 日 14:13 UTC
- 編集日時: 2022 年 11 月 17 日 00:56 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonNimbleStudio-LaunchProfileWorker

AmazonNimbleStudio-LaunchProfileWorker は、Nimble Studio 起動プロファイルワーカーが必要とするリソースへのアクセス権を付与する AWS マネージドポリシーです。Nimble Studio Builder で作成された EC2 インスタンスにこのポリシーをアタッチします。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonNimbleStudio-LaunchProfileWorker をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 4 月 28 日 04:47 UTC
- 編集日時: 2021 年 4 月 28 日 04:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonNimbleStudio-StudioAdmin

AmazonNimbleStudio-StudioAdmin は、スタジオ管理者に関連付けられた Amazon Nimble Studio リソースと、他のサービスの関連するスタジオリソースへのアクセス権を付与する AWS マネージドポリシーです。このポリシーをスタジオに関連する管理者ロールにアタッチしてください。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonNimbleStudio-StudioAdmin をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 4 月 28 日 04:47 UTC
- 編集日時: 2023 年 9 月 22 日 17:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonNimbleStudio-StudioUser

AmazonNimbleStudio-StudioUser は、スタジオユーザーに関連付けられた Amazon Nimble Studio リソースと、他のサービスの関連するスタジオリソースへのアクセス権を付与する AWS マネージドポリシーです。このポリシーをスタジオに関連付けられているユーザーロールにアタッチしてください。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonNimbleStudio-StudioUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 4 月 28 日 04:48 UTC
- 編集日時: 2023 年 9 月 22 日 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonOmicsFullAccess

AmazonOmicsFullAccess は、Amazon Omics とその他の必要な AWS のサービス へのフルアクセスを提供する AWS マネージドポリシーです。このポリシーにより、ユーザーは RAM 共有の招待を表示して承諾し、ユーザーの AWS アカウント 以外のリソースにアクセスすることができます。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOmicsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 2 月 24 日 00:59 UTC

- 編集日時: 2023 年 2 月 24 日 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonOmicsReadOnlyAccess

`AmazonOmicsReadOnlyAccess` は、Amazon Omics への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonOmicsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 29 日 04:17 UTC
- 編集日時: 2022 年 11 月 29 日 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonOneEnterpriseFullAccess

`AmazonOneEnterpriseFullAccess`は、AWS次のような管理ポリシーです。このポリシーは、Amazon One Enterprise のすべてのリソースとオペレーションへのアクセスを許可する管理権限を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonOneEnterpriseFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時間:2023 年 11 月 28 日 04:58 UTC

- 編集時間:2023 年 11 月 28 日 04:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonOneEnterpriseInstallerAccess

AmazonOneEnterpriseInstallerAccessAWSは次のような管理ポリシーです。このポリシーは、デバイスのインストールとアクティベーションを許可する限定的な読み取りおよび書き込み権限を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOneEnterpriseInstallerAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時間:2023 年 11 月 28 日 05:00 UTC
- 編集時間:2023 年 11 月 28 日 05:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
```

```
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonOneEnterpriseReadOnlyAccess

`AmazonOneEnterpriseReadOnlyAccess`AWSは次のような管理ポリシーです。このポリシーは、Amazon One Enterprise のすべてのリソースとオペレーションに読み取り専用アクセス権限を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonOneEnterpriseReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時間:2023 年 11 月 28 日 04:59 UTC
- 編集時間:2023 年 11 月 28 日 04:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonOpenSearchDashboardsServiceRolePolicy

`AmazonOpenSearchDashboardsServiceRolePolicy`は、Amazon OpenSearch Dashboards Service へのアクセスを提供して、AWSAWS CloudWatch ユーザーに代わって他のサービスにアクセスできるようにする管理ポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成時間:2023 年 12 月 22 日 19:38 UTC
- 編集時間:2023 年 12 月 22 日 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonOpenSearchIngestionFullAccess

AmazonOpenSearchIngestionFullAccess は、Amazon OpenSearch Ingestion がユーザーに代わって他の AWS サービスにアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOpenSearchIngestionFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 4 月 26 日 18:11 UTC
- 編集日時: 2023 年 4 月 26 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonOpenSearchIngestionReadOnlyAccess

AmazonOpenSearchIngestionReadOnlyAccess は、Amazon OpenSearch Ingestion Service への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOpenSearchIngestionReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 4 月 26 日 18:09 UTC
- 編集日時: 2023 年 4 月 26 日 18:09 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource"
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonOpenSearchIngestionServiceRolePolicy

`AmazonOpenSearchIngestionServiceRolePolicy` は、Amazon OpenSearch Ingestion Service がユーザーに代わって他の AWS サービスにアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 18 日 16:49 UTC
- 編集日時: 2022 年 11 月 18 日 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonOpenSearchServerlessServiceRolePolicy

AmazonOpenSearchServerlessServiceRolePolicy は、Amazon OpenSearch Serverless がユーザーに代わって CloudWatch API などの他の AWS サービスにアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 24 日 19:50 UTC
- 編集日時: 2022 年 11 月 24 日 19:50 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AOSS"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonOpenSearchServiceCognitoAccess

AmazonOpenSearchServiceCognitoAccess は、Amazon Cognito 設定サービスへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOpenSearchServiceCognitoAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 9 月 2 日 06:31 UTC
- 編集日時: 2021 年 12 月 20 日 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
```

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonOpenSearchServiceFullAccess

AmazonOpenSearchServiceFullAccess は、Amazon OpenSearch Service 設定サービスへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOpenSearchServiceFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 9 月 8 日 05:33 UTC
- 編集日時: 2021 年 9 月 8 日 05:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonOpenSearchServiceReadOnlyAccess

`AmazonOpenSearchServiceReadOnlyAccess` は、Amazon OpenSearch Service 設定サービスへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonOpenSearchServiceReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 9 月 8 日 05:38 UTC
- 編集日時: 2021 年 9 月 8 日 05:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonOpenSearchServiceRolePolicy

`AmazonOpenSearchServiceRolePolicy` は、Amazon OpenSearch Service がユーザーに代わって EC2 ネットワーク API などの他の AWS サービスにアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 8 月 26 日 09:27 UTC
- 編集日時: 2023 年 10 月 23 日 07:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
```

```
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonPersonalizeFullAccess

`AmazonPersonalizeFullAccess` は、AWS Management Console および SDK を使用して Amazon Personalize へのフルアクセスを提供する AWS マネージドポリシーです。関連サービス (S3、CloudWatch など) への限定アクセスも提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonPersonalizeFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 12 月 4 日 22:24 UTC
- 編集日時: 2019 年 5 月 30 日 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonPollyFullAccess

AmazonPollyFullAccess は、Amazon Polly のサービスとリソースへのフルアクセス権を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonPollyFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 11 月 30 日 18:59 UTC
- 編集日時: 2016 年 11 月 30 日 18:59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPollyFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Effect" : "Allow",
      "Action" : [
        "polly:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonPollyReadOnlyAccess

`AmazonPollyReadOnlyAccess` は、Amazon Polly リソースへの読み取り専用アクセス権を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonPollyReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 11 月 30 日 18:59 UTC
- 編集日時: 2018 年 7 月 17 日 16:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonPrometheusConsoleFullAccess

`AmazonPrometheusConsoleFullAccess` は、AWS コンソールで AWS Managed Prometheus リソースへのフルアクセス権を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonPrometheusConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 15 日 18:11 UTC
- 編集日時: 2022 年 10 月 24 日 22:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonPrometheusFullAccess

`AmazonPrometheusFullAccess` は、AWS Managed Prometheus リソースへのフルアクセス権を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonPrometheusFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 15 日 18:10 UTC
- 編集時間:2023 年 11 月 26 日 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonPrometheusQueryAccess

`AmazonPrometheusQueryAccess` は、AWS Managed Prometheus リソースに対してクエリを実行するためのアクセス権を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonPrometheusQueryAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2020 年 12 月 19 日 01:02 UTC
- 編集日時: 2020 年 12 月 19 日 01:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonPrometheusRemoteWriteAccess

AmazonPrometheusRemoteWriteAccess は、AWS Managed Prometheus ワークスペースへの書き込み専用アクセス権を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonPrometheusRemoteWriteAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 19 日 01:04 UTC
- 編集日時: 2020 年 12 月 19 日 01:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonPrometheusScraperServiceRolePolicy

AmazonPrometheusScraperServiceRolePolicyは、Amazon AWSAWSマネージドサービスが管理または使用するリソースへのアクセスをPrometheus Collector に提供する管理ポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成時間:2023 年 11 月 26 日 14:19 UTC
- 編集時間:2023 年 11 月 26 日 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScraperServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonQFullAccess

AmazonQFullAccessは、AWS次のような管理ポリシーです。Amazon Q とのやりとりを可能にするフルアクセスを提供します

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonQFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時間:2023 年 11 月 28 日 16:00 UTC
- 編集時間:2023 年 11 月 28 日 16:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Effect" : "Allow",
      "Action" : [
        "q:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonQLDBConsoleFullAccess

AmazonQLDBConsoleFullAccess は、AWS Management Console 経由で Amazon QLDB へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonQLDBConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 9 月 5 日 18:24 UTC
- 編集日時: 2022 年 11 月 4 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonQLDBFullAccess

AmazonQLDBFullAccess は、サービス API 経由で Amazon QLDB へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonQLDBFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 9 月 5 日 18:23 UTC
- 編集日時: 2022 年 11 月 4 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonQLDBReadOnly

AmazonQLDBReadOnly は、Amazon QLDB への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonQLDBReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 9 月 5 日 18:19 UTC
- 編集日時: 2021 年 7 月 2 日 02:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBReadOnly

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRDSBetaServiceRolePolicy

`AmazonRDSBetaServiceRolePolicy` は、Amazon RDS がユーザーに代わって AWS リソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 5 月 2 日 19:41 UTC
- 編集日時: 2022 年 12 月 14 日 18:33 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRDSCustomInstanceProfileRolePolicy

AmazonRDSCustomInstanceProfileRolePolicy は、Amazon RDS Custom が EC2 インスタンスプロファイルを介してさまざまなオートメーションアクションとデータベース管理タスクを実行できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRDSCustomInstanceProfileRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時刻: 2024 年 2 月 27 日 17:42 UTC
- 編集日時： 2024 年 2 月 27 日 17:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonRDSCustomPreviewServiceRolePolicy

AmazonRDSCustomPreviewServiceRolePolicy は、Amazon RDS Custom プレビューサービスロールポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 10 月 8 日 21:44 UTC
- 編集日時: 2023 年 9 月 20 日 17:48 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRDSCustomServiceRolePolicy

AmazonRDSCustomServiceRolePolicy は、Amazon RDS Custom がユーザーに代わって AWS リソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 10 月 8 日 21:39 UTC
- 編集日時: 2023 年 9 月 20 日 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRDSDataFullAccess

AmazonRDSDataFullAccess は、RDS データ API、RDS データベース認証情報用のシークレットストア API、および DB コンソールクエリ管理 API を使用して、AWS アカウント 内の Aurora Serverless クラスターで SQL ステートメントを実行するためのフルアクセスをできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRDSDataFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 20 日 21:29 UTC
- 編集日時: 2019 年 11 月 20 日 21:58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSDataFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRDSDirectoryServiceAccess

AmazonRDSDirectoryServiceAccess は、ドメインに参加している SQL Server DB インスタンスについて、お客様に代わって RDS が Directory Service マネージド AD にアクセスできるようにする AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRDSDirectoryServiceAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 2 月 26 日 02:02 UTC
- 編集日時: 2019 年 5 月 15 日 16:51 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRDSEnhancedMonitoringRole

AmazonRDSEnhancedMonitoringRole は、RDS 拡張モニタリング用 CloudWatch にアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRDSEnhancedMonitoringRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 11 月 11 日 19:58 UTC
- 編集日時: 2015 年 11 月 11 日 19:58 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRDSFullAccess

`AmazonRDSFullAccess` は、AWS Management Console 経由で Amazon RDS へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRDSFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2023 年 8 月 17 日 23:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRDSPerformanceInsightsFullAccess

`AmazonRDSPerformanceInsightsFullAccess` は、AWS Management Console 経由で RDS Performance Insights へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRDSPerformanceInsightsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 8 月 15 日 23:41 UTC
- 編集日時: 2023 年 10 月 23 日 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRDSPerformanceInsightsReadOnly

`AmazonRDSPerformanceInsightsReadOnly` は、RDS Performance Insights 用の読み取り専用 AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRDSPerformanceInsightsReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 4 月 5 日 00:02 UTC

- 編集日時: 2023 年 10 月 23 日 21:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRDSPreviewServiceRolePolicy

AmazonRDSPreviewServiceRolePolicy は、Amazon RDS プレビューサービスロールポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 5 月 31 日 18:02 UTC
- 編集日時: 2023 年 10 月 4 日 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "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"
        }
      }
    }
  ]
```

```
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRDSReadOnlyAccess

AmazonRDSReadOnlyAccess は、AWS Management Console 経由で Amazon RDS への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRDSReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2023 年 4 月 14 日 12:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRDSServiceRolePolicy

`AmazonRDSServiceRolePolicy` は、Amazon RDS がユーザーに代わって AWS リソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 1 月 8 日 18:17 UTC
- 編集日時： 2024 年 1 月 19 日 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v13 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRedshiftAllCommandsFullAccess

AmazonRedshiftAllCommandsFullAccess は、Amazon Redshift のデータをコピー、ロード、アンロード、クエリ、分析するための SQL コマンドを実行するアクセス許可を含む AWS マネージドポリシーです。また、このポリシーでは、関連するサービス (Amazon S3、Amazon CloudWatch Logs、Amazon SageMaker、AWS Glue など) 用のいくつかのステートメントを実行するアクセス許可も付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftAllCommandsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 4 日 00:48 UTC
- 編集日時: 2021 年 11 月 25 日 02:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRedshiftDataFullAccess

AmazonRedshiftDataFullAccess は、Amazon Redshift Data API へのフルアクセスを提供する AWS マネージドポリシーです。このポリシーは、その他の必要なサービスへのスコープ付きアクセスも付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftDataFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 9 月 9 日 19:23 UTC
- 編集日時: 2023 年 4 月 7 日 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRedshiftFullAccess

AmazonRedshiftFullAccess は、AWS Management Console 経由で Amazon Redshift へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2022 年 7 月 7 日 23:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRedshiftQueryEditor

`AmazonRedshiftQueryEditor` は、Amazon Redshift クエリエディタへのフルアクセスと、AWS Management Console 経由で保存されたクエリへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftQueryEditor をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 10 月 4 日 22:50 UTC
- 編集日時: 2021 年 2 月 16 日 19:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRedshiftQueryEditorV2FullAccess

AmazonRedshiftQueryEditorV2FullAccess は、Amazon Redshift クエリエディタ V2 オペレーションとリソースへのフルアクセス権を付与する AWS マネージドポリシーです。このポリシーは、その他の必要なサービスへのアクセス権限も付与します。これには、 AWS KMS で Amazon Redshift クラスター、読み取りキー、エイリアスを一覧表示し、 AWS Secrets Manager でクエリエディタ V2 シークレットを管理するアクセス許可が含まれます。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftQueryEditorV2FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 9 月 24 日 14:06 UTC

- 編集日時： 2024 年 2 月 21 日 17:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonRedshiftQueryEditorV2NoSharing

`AmazonRedshiftQueryEditorV2NoSharing` は、リソースを共有せずに Amazon Redshift クエリエディタ V2 を操作する権限を付与する AWS マネージドポリシーです。権限を与えられたプリンシパルは、そのリソースの読み取り、更新、削除のみが可能で、共有はできません。このポリシーは、その他の必要なサービスへのアクセス権限も付与します。これには、Amazon Redshift クラス

ターを一覧表示し、 AWS Secrets Manager でプリンシパルのクエリエディタ V2 シークレットを管理するアクセス許可が含まれます。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftQueryEditorV2NoSharing をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 9 月 24 日 14:18 UTC
- 編集日時： 2024 年 2 月 21 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonRedshiftQueryEditorV2ReadSharing

`AmazonRedshiftQueryEditorV2ReadSharing` は、リソース共有を限定して Amazon Redshift クエリエディタ V2 を操作する権限を付与する AWS マネージドポリシーです。付与されたプリンシパルは、そのリソースを読み取り、書き込み、共有することができます。付与されたプリンシパルは、チームと共有されているリソースの読み取りはできますが、更新はできません。このポリシーは、その他の必要なサービスへのアクセス権限も付与します。これには、Amazon Redshift クラスターを一覧表示し、 AWS Secrets Manager でプリンシパルのクエリエディタ V2 シークレットを管理するアクセス許可が含まれます。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRedshiftQueryEditorV2ReadSharing` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 9 月 24 日 14:22 UTC
- 編集日時： 2024 年 2 月 21 日 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing`

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonRedshiftQueryEditorV2ReadWriteSharing

AmazonRedshiftQueryEditorV2ReadWriteSharing は、リソースを共有して Amazon Redshift クエリエディタ v2 を操作する権限を付与する AWS マネージドポリシーです。付与されたプリンシパルは、そのリソースを読み取り、書き込み、共有することができます。付与されたプリンシパルは、そのチームと共有されているリソースを読み取り、更新することができます。このポリシーは、その他の必要なサービスへのアクセス権限も付与します。これには、Amazon Redshift クラスターを一覧表示し、 AWS Secrets Manager でプリンシパルのクエリエディタ V2 シークレットを管理するアクセス許可が含まれます。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftQueryEditorV2ReadWriteSharing をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 9 月 24 日 14:25 UTC
- 編集日時： 2024 年 2 月 21 日 17:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonRedshiftReadOnlyAccess

AmazonRedshiftReadOnlyAccess は、経由で Amazon Redshift への読み取り専用アクセスを提供する AWS マネージドポリシーです AWS Management Console。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時： 2024 年 2 月 8 日 00:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonRedshiftServiceLinkedRolePolicy

`AmazonRedshiftServiceLinkedRolePolicy` は、Amazon Redshift がユーザーに代わって AWS サービスを呼び出すことを許可する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 18 日 19:19 UTC
- 編集日時： 2024 年 3 月 15 日 20:00 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v13 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonRekognitionCustomLabelsFullAccess

AmazonRekognitionCustomLabelsFullAccess は、Amazon Rekognition Custom Labels 機能に必要な rekognition と S3 のアクセス許可を指定する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRekognitionCustomLabelsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 1 月 8 日 19:18 UTC
- 編集日時: 2022 年 8 月 16 日 20:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRekognitionFullAccess

AmazonRekognitionFullAccess は、すべての Amazon Rekognition API にアクセスする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRekognitionFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 11 月 30 日 14:40 UTC
- 編集日時: 2016 年 11 月 30 日 14:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRekognitionReadOnlyAccess

AmazonRekognitionReadOnlyAccess は、すべての読み取り rekognition API にアクセスする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRekognitionReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 11 月 30 日 14:58 UTC
- 編集日時: 2023 年 11 月 8 日 18:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRekognitionServiceRole

AmazonRekognitionServiceRole は、Rekognition がユーザーに代わって AWS サービスを呼び出せるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRekognitionServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 11 月 29 日 16:52 UTC
- 編集日時: 2017 年 11 月 29 日 16:52 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRoute53AutoNamingFullAccess

AmazonRoute53AutoNamingFullAccess は、Route 53 のすべての自動命名アクションへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53AutoNamingFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 1 月 18 日 18:40 UTC
- 編集日時: 2018 年 1 月 18 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRoute53AutoNamingReadOnlyAccess

AmazonRoute53AutoNamingReadOnlyAccess は、Route 53 のすべての自動命名アクションへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53AutoNamingReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 1 月 18 日 03:02 UTC
- 編集日時: 2018 年 1 月 18 日 03:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRoute53AutoNamingRegistrantAccess

AmazonRoute53AutoNamingRegistrantAccess は、Route 53 自動命名アクションへの登録者レベルのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53AutoNamingRegistrantAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 3 月 12 日 22:33 UTC
- 編集日時: 2018 年 3 月 12 日 22:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRoute53DomainsFullAccess

AmazonRoute53DomainsFullAccess は、Route53 Domains のすべてのアクションへのフルアクセスを提供し、ドメイン登録の一環としてホストゾーンを作成できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53DomainsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRoute53DomainsReadOnlyAccess

`AmazonRoute53DomainsReadOnlyAccess` は、Route53 ドメインのリストとアクションへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRoute53DomainsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRoute53FullAccess

AmazonRoute53FullAccess は、AWS Management Console 経由ですべての Amazon Route 53 へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2018 年 12 月 20 日 21:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53FullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRoute53ReadOnlyAccess

`AmazonRoute53ReadOnlyAccess` は、AWS Management Console 経由ですべての Amazon Route 53 への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRoute53ReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2016 年 11 月 15 日 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRoute53RecoveryClusterFullAccess

AmazonRoute53RecoveryClusterFullAccess は、Amazon Route 53 リカバリクラスターへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53RecoveryClusterFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 8 月 18 日 18:37 UTC
- 編集日時: 2021 年 8 月 18 日 18:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRoute53RecoveryClusterReadOnlyAccess

`AmazonRoute53RecoveryClusterReadOnlyAccess` は、Amazon Route 53 リカバリクラスターへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRoute53RecoveryClusterReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 8 月 18 日 17:36 UTC
- 編集日時: 2022 年 4 月 1 日 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRoute53RecoveryControlConfigFullAccess

AmazonRoute53RecoveryControlConfigFullAccess は、Amazon Route 53 リカバリコントロール 設定へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53RecoveryControlConfigFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 8 月 18 日 17:48 UTC
- 編集日時: 2021 年 8 月 18 日 17:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRoute53RecoveryControlConfigReadOnlyAccess

AmazonRoute53RecoveryControlConfigReadOnlyAccess は、Amazon Route 53 リカバリコントロール 設定への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53RecoveryControlConfigReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 8 月 18 日 18:01 UTC
- 編集日時: 2023 年 10 月 18 日 17:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRoute53RecoveryReadinessFullAccess

`AmazonRoute53RecoveryReadinessFullAccess` は、Amazon Route 53 のリカバリの準備状況へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRoute53RecoveryReadinessFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 8 月 18 日 16:45 UTC
- 編集日時: 2021 年 8 月 18 日 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRoute53RecoveryReadinessReadOnlyAccess

AmazonRoute53RecoveryReadinessReadOnlyAccess は、Amazon Route 53 のリカバリの準備状況への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53RecoveryReadinessReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 8 月 18 日 18:11 UTC
- 編集日時: 2021 年 11 月 9 日 20:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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::*:*"
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRoute53ResolverFullAccess

`AmazonRoute53ResolverFullAccess` は、Route 53 Resolver のフルアクセスポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonRoute53ResolverFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 5 月 30 日 18:10 UTC
- 編集日時: 2020 年 7 月 17 日 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonRoute53ResolverReadOnlyAccess

AmazonRoute53ResolverReadOnlyAccess は、Route 53 Resolver の読み取り専用ポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53ResolverReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 5 月 30 日 18:11 UTC
- 編集日時: 2019 年 9 月 27 日 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonS3FullAccess

AmazonS3FullAccess は、AWS Management Console 経由ですべてのバケットへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonS3FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2021 年 9 月 27 日 20:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3FullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:*",
```

```
        "s3-object-lambda:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonS3ObjectLambdaExecutionRolePolicy

AmazonS3ObjectLambdaExecutionRolePolicy は、Amazon S3 Object Lambda と対話するためのアクセス許可を AWS Lambda 関数に提供する AWS マネージドポリシーです。また、Amazon CloudWatch Logs に書き込むアクセス許可を Lambda に付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonS3ObjectLambdaExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 8 月 18 日 10:07 UTC
- 編集日時: 2021 年 8 月 18 日 10:07 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonS3OutpostsFullAccess

`AmazonS3OutpostsFullAccess` は、AWS Management Console 経由で Outposts の Amazon S3 へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonS3OutpostsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 10 月 2 日 17:26 UTC
- 編集日時: 2020 年 10 月 2 日 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonS3OutpostsReadOnlyAccess

`AmazonS3OutpostsReadOnlyAccess` は、AWS Management Console 経由で Outposts の Amazon S3 への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonS3OutpostsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 10 月 2 日 18:55 UTC
- 編集日時: 2020 年 10 月 2 日 18:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonS3ReadOnlyAccess

`AmazonS3ReadOnlyAccess` は、AWS Management Console 経由ですべてのバケットへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonS3ReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2023 年 8 月 10 日 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

`AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy` は、Amazon SageMaker 製品ポートフォリオから製品をプロビジョニングするために AWS のサービスカタログサービスが使用するサービスロールポリシーである AWS マネージドポリシーです。CodePipeline、CodeBuild、CodeCommit、Glue、CloudFormation などの一連の関連サービスにアクセス許可を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 11 月 27 日 18:48 UTC
- 編集日時: 2022 年 8 月 2 日 19:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerCanvasAIServicesAccess

AmazonSageMakerCanvasAIServicesAccessは、Amazon SageMaker Canvas に AI サービスを使用する権限を付与し、すぐに使用できる AI AWSソリューションをサポートするための管理ポリシーです。このポリシーでは、Amazon SageMaker Canvas がサポートを追加するにつれて、サービスに対する変更権限がさらに追加されます。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerCanvasAIServicesAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 3 月 23 日 22:36 UTC
- 編集時間:2023 年 11 月 29 日 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerCanvasBedrockAccess

AmazonSageMakerCanvasBedrockAccess は、S3 などのダウンストリームサービスへのアクセスを提供することで、Canvas SageMaker で Amazon Bedrock を使用するアクセス許可を付与するAWSマネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerCanvasBedrockAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成時刻: 2024 年 2 月 2 日 18:37 UTC
- 編集日時： 2024 年 2 月 2 日 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
      ]
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerCanvasDataPrepFullAccess

AmazonSageMakerCanvasDataPrepFullAccessは、Canvas でのデータ準備のための Amazon AWS SageMaker リソースとオペレーションへのフルアクセスを提供する管理ポリシーです。このポリシーでは、関連サービス (S3、IAM、KMS、RDS、 CloudWatch ログ、Redshift、Athena、Glue、EventBridge Secrets Manager など) への特定のアクセスも提供されます。このポリシーは Amazon SageMaker ドメイン/ユーザープロファイル実行ロールに添付する必要があります。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerCanvasDataPrepFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 10 月 27 日 22:56 UTC
- 編集時間:2023 年 12 月 8 日 02:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerCanvasDirectDeployAccess

AmazonSageMakerCanvasDirectDeployAccessは、Amazon SageMaker Canvas が Canvas を通じて作成されたエンドポイントのエンドポイント詳細を作成、管理、表示できるようにする AWS マネージドポリシーです。Amazon SageMaker Canvas が CloudWatch からエンドポイント呼び出しメトリクスを取得できるようにします。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerCanvasDirectDeployAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 10 月 6 日 18:11 UTC
- 編集日時: 2023 年 10 月 6 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerCanvasForecastAccess

AmazonSageMakerCanvasForecastAccessは、SageMaker Canvas を Amazon Forecast で使用するために一般的に必要となるアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerCanvasForecastAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 8 月 24 日 20:04 UTC
- 編集日時: 2022 年 8 月 24 日 20:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerCanvasFullAccess

AmazonSageMakerCanvasFullAccess は、Amazon SageMaker Canvas のリソースとオペレーションへのフルアクセスを提供する AWSマネージドポリシーです。このポリシーは、関連サービス (S3、IAM、VPC、ECR、 CloudWatch Logs、Redshift、Secrets Manager、Forecast など) への選択アクセスも提供します。このポリシーは、Amazon SageMaker ドメイン/ユーザープロファイル実行ロールにアタッチする必要があります。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerCanvasFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 9 月 9 日 00:44 UTC

- 編集日時： 2024 年 1 月 24 日 22:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerClusterInstanceRolePolicy

`AmazonSageMakerClusterInstanceRolePolicy`は、AWS次のような管理ポリシーです。このポリシーは、Amazon SageMaker Cluster を使用するために一般的に必要とされるアクセス権限を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerClusterInstanceRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時間:2023 年 11 月 29 日 15:11 UTC
- 編集時間:2023 年 11 月 29 日 15:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerCoreServiceRolePolicy

AmazonSageMakerCoreServiceRolePolicy は、Amazon SageMaker コアサービスのサービスリンクロールのマネージドポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 21 日 21:40 UTC
- 編集日時: 2020 年 12 月 21 日 21:40 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerEdgeDeviceFleetPolicy

AmazonSageMakerEdgeDeviceFleetPolicy は、SageMaker Edge がデフォルトのクラウド接続を使用して顧客のデバイスフリートを作成および管理するために必要なアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerEdgeDeviceFleetPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 8 日 16:17 UTC
- 編集日時: 2020 年 12 月 8 日 16:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerFeatureStoreAccess

AmazonSageMakerFeatureStoreAccess は、Amazon SageMaker FeatureStore 機能グループのオフラインストアを有効にするために必要なアクセス権限を提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerFeatureStoreAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 1 日 16:24 UTC
- 編集日時: 2022 年 12 月 5 日 14:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerFullAccess

AmazonSageMakerFullAccessは、AWS Management Consoleおよび SDK SageMaker を使用して Amazon AWSへのフルアクセスを提供する管理ポリシーです。また、関連サービス (S3、ECR、CloudWatch ログなど) への特定のアクセスも提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 29 日 13:07 UTC
- 編集時間:2023 年 11 月 30 日 13:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v25 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerGeospatialExecutionRole

AmazonSageMakerGeospatialExecutionRole は、SageMaker Geospatial を使用するために一般的に必要とされるサービスへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerGeospatialExecutionRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 11 月 30 日 10:08 UTC
- 編集日時: 2023 年 5 月 10 日 20:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerGeospatialFullAccess

`AmazonSageMakerGeospatialFullAccess` は、AWS Management Console および SDK 経由で Amazon SageMaker Geospatial へのフルアクセスを許可するアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerGeospatialFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2022 年 11 月 30 日 10:06 UTC
- 編集日時: 2022 年 11 月 30 日 10:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerGroundTruthExecution

AmazonSageMakerGroundTruthExecution は、SageMaker GroundTruth Labeling ジョブの実行に必要な AWS サービスへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerGroundTruthExecution をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 7 月 9 日 19:30 UTC
- 編集日時: 2022 年 4 月 29 日 20:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerMechanicalTurkAccess

AmazonSageMakerMechanicalTurkAccessは、任意のワークチームに対して Amazon Augmented AI FlowDefinition リソースを作成するためのアクセスを提供する AWSマネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerMechanicalTurkAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 3 日 16:19 UTC
- 編集日時: 2019 年 12 月 3 日 16:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerModelGovernanceUseAccess

`AmazonSageMakerModelGovernanceUseAccess`は、次のような AWS マネージドポリシーです。この AWS マネージドポリシーは、Amazon SageMaker ガバナンス機能のすべてを使用するために必要なアクセス権限を付与します。このポリシーは、関連サービス (S3、KMS など) への限定アクセスも提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerModelGovernanceUseAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 30 日 08:58 UTC
- 編集日時: 2023 年 7 月 17 日 22:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerModelRegistryFullAccess

AmazonSageMakerModelRegistryFullAccessは、Sagemaker のモデルレジストリ用の新しいマネージドポリシーである AWS マネージドポリシーです。このポリシーは、ユーザーロールにアタッチして Sagemaker のモデルレジストリ関連の機能にアクセスできるスタンドアロンポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerModelRegistryFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 4 月 13 日 05:20 UTC
- 編集日時: 2023 年 4 月 13 日 05:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
```

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerNotebooksServiceRolePolicy

AmazonSageMakerNotebooksServiceRolePolicy は、Amazon SageMaker ノートブックのサービスリンクロールのマネージドポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 10 月 18 日 20:27 UTC
- 編集日時: 2023 年 3 月 9 日 18:20 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
```

```
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceR

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy は、Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内で、AWS APIGateway が使用するサービスロールポリシーである AWS マネージドポリシーです。Lambda などを含む一連の関連サービスにアクセス許可を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 8 月 1 日 15:06 UTC
- 編集日時: 2023 年 8 月 1 日 15:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServi

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy は、Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内で、AWS CloudFormation が使用するサービスロールポリシーである AWS マネージドポリシーです。Lambda、APIGateway などの関連サービスのサブセットにアクセス許可を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 8 月 1 日 15:06 UTC
- 編集日時: 2023 年 8 月 1 日 15:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRoleP

`AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy` は、Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内で、AWS Lambda が使用するサービスロールポリシーである AWS マネージドポリシーです。Secrets Manager などを含む一連の関連サービスにアクセス許可を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 8 月 1 日 15:05 UTC
- 編集日時: 2023 年 8 月 1 日 15:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerPipelinesIntegrations

AmazonSageMakerPipelinesIntegrations は、次のような AWS マネージドポリシーです。この Amazon マネージドポリシーは、SageMaker モデル構築パイプラインのコールバックステップと Lambda ステップでの使用に一般的に必要なアクセス許可を付与します。SageMaker Studio のセットアップ時に作成できる AmazonSageMaker-ExecutionRole に追加されます。パイプラインの作成または実行に使用される他のロールにアタッチすることもできます。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerPipelinesIntegrations をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 7 月 30 日 16:35 UTC
- 編集日時: 2023 年 2 月 17 日 21:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerReadOnly

`AmazonSageMakerReadOnly` は、AWS Management Console および SDK 経由で Amazon SageMaker への読み取り専用アクセス権を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 29 日 13:07 UTC
- 編集日時: 2021 年 12 月 1 日 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePoli

`AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy` は、Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内で、AWS APIGateway が使用するサービスロールポリシーである AWS マネージドポリシーです。CloudWatch Logs やその他の関連サービスのセットにアクセス許可を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 3 月 25 日 04:25 UTC
- 編集日時: 2022 年 3 月 25 日 04:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerServiceCatalogProductsCloudformationServiceRoleP

`AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy` は、Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内で、AWS CloudFormation が使用するサービスロールポリシーである AWS マネージドポリシーです。SageMaker やその他の関連サービスの一部にアクセス許可を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 3 月 25 日 04:26 UTC

- 編集日時: 2022 年 3 月 25 日 04:26 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

`AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy` は、Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内の AWS CodeBuild が使用するサービスロールポリシーである AWS マネージドポリシーです。CodePipeline、CodeBuild などを含む関連サービスのサブセットにアクセス許可を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 3 月 25 日 04:27 UTC
- 編集日時: 2022 年 3 月 25 日 04:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

`AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy` は、Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内の AWS CodePipeline によって使用されるサービスロールポリシーである AWS マネージドポリシーです。CodePipeline、CodeBuild などを含む関連サービスのサブセットにアクセス許可を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 2 月 22 日 09:53 UTC
- 編集日時: 2022 年 2 月 22 日 09:53 UTC

- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy は AWS マネージドポリシーです。Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内の AWS CloudWatch イベントによって使用されるサービスロールポリシーです。CodePipeline やその他を含む関連サービスのサブセットにアクセス許可を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 2 月 22 日 09:53 UTC
- 編集日時: 2022 年 2 月 22 日 09:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Action" : "codepipeline:StartPipelineExecution",
      "Resource" : "arn:aws:codepipeline:*:*:sagemaker-*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy は AWS マネージドポリシーです。Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内で AWS Firehose が使用するサービスロールポリシーです。Firehose などを含む一連の関連サービスにアクセス許可を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 2 月 22 日 09:54 UTC
- 編集日時: 2022 年 2 月 22 日 09:54 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

`AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy` は AWS マネージドポリシーです。Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内の AWS Glue が使用するサービスロールポリシーです。このポリシーは、Glue やその他を含めた一連の関連サービスにアクセス許可を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 2 月 22 日 09:51 UTC
- 編集日時: 2022 年 8 月 26 日 19:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy は、Amazon SageMaker 製品ポートフォリオの AWS ServiceCatalog プロビジョニング製品内で、AWS Lambda が使用するサービスロールポリシーである AWS マネージドポリシーです。ECR、S3、その他を含む一連の関連サービスにアクセス許可を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 4 月 4 日 16:34 UTC
- 編集日時: 2022 年 4 月 4 日 16:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSecurityLakeAdministrator

AmazonSecurityLakeAdministrator は、Amazon Security Lake と、Security Lake の管理に必要な関連サービスへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSecurityLakeAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 5 月 30 日 22:04 UTC
- 編集日時： 2024 年 2 月 23 日 16:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonSecurityLakeMetastoreManager

`AmazonSecurityLakeMetastoreManager` は、cloudwatch、S3、 Glue、および SQS へのアクセスを許可する Amazon SecurityLake メタストアマネージャー Lambda の AWSマネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSecurityLakeMetastoreManager` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成時刻: 2024 年 1 月 23 日 15:26 UTC
- 編集日時： 2024 年 1 月 23 日 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
```

```
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSecurityLakePermissionsBoundary

AmazonSecurityLakePermissionsBoundary は、次のような AWS マネージドポリシーです。Amazon Security Lake は、サードパーティのカスタムソースがデータレイクにデータを書き込むために、およびサードパーティのサブスクライバーがデータレイクからデータを消費するための IAM ロールを作成し、ロールを作成する際にこのポリシーを使用して権限の境界を定義します。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSecurityLakePermissionsBoundary をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 29 日 14:11 UTC
- 編集日時: 2022 年 11 月 29 日 14:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSESFullAccess

`AmazonSESFullAccess` は、AWS Management Console 経由で Amazon SES へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSESFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSESReadOnlyAccess

`AmazonSESReadOnlyAccess` は、AWS Management Console 経由で Amazon SES への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSESReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSNSFullAccess

`AmazonSNSFullAccess` は、AWS Management Console 経由で Amazon SNS へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSNSFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSNSReadOnlyAccess

`AmazonSNSReadOnlyAccess` は、AWS Management Console 経由で Amazon SNS への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSNSReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSNSRole

AmazonSNSRole は、Amazon SNS サービスロールのデフォルトポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSNSRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSNSRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSQSFullAccess

`AmazonSQSFullAccess` は、AWS Management Console 経由で Amazon SQS へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSQSFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSQSReadOnlyAccess

`AmazonSQSReadOnlyAccess` は、AWS Management Console 経由で Amazon SQS への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSQSReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2023 年 6 月 15 日 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSSMAutomationApproverAccess

AmazonSSMAutomationApproverAccess は、、自動化実行の表示と、承認待ちの自動化に対する承認決定の送信のアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMAutomationApproverAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 8 月 7 日 23:07 UTC
- 編集日時: 2017 年 8 月 7 日 23:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationExecutions",
        "ssm:GetAutomationExecution",
        "ssm:SendAutomationSignal"
      ],
      "Resource" : [
```

```
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSSMAutomationRole

AmazonSSMAutomationRole は、EC2 Automation Service に、自動化ドキュメント内で定義されたアクティビティを実行する権限を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMAutomationRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 12 月 5 日 22:09 UTC
- 編集日時: 2017 年 7 月 24 日 23:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSSMDirectoryServiceAccess

`AmazonSSMDirectoryServiceAccess` は、SSM エージェントは顧客に代わって Directory Service にアクセスし、マネージドインスタンスをドメインに参加させることを可能にする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSSMDirectoryServiceAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2019 年 3 月 15 日 17:44 UTC
- 編集日時: 2019 年 3 月 15 日 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSSMFullAccess

AmazonSSMFullAccess は、Amazon SSM へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 5 月 29 日 17:39 UTC
- 編集日時: 2019 年 11 月 20 日 20:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSSMMaintenanceWindowRole

AmazonSSMMaintenanceWindowRole は、EC2 メンテナンスウィンドウに使用するサービスロールである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMMaintenanceWindowRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 12 月 1 日 15:57 UTC
- 編集日時: 2019 年 7 月 27 日 00:16 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSSMManagedEC2InstanceDefaultPolicy

`AmazonSSMManagedEC2InstanceDefaultPolicy` は、EC2 インスタンスで AWS Systems Manager 機能を有効にする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSSMManagedEC2InstanceDefaultPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 8 月 30 日 20:54 UTC
- 編集日時: 2022 年 8 月 30 日 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSSMManagedInstanceCore

`AmazonSSMManagedInstanceCore` は、AWS Systems Manager サービスのコア機能を有効にするための Amazon EC2 ロール用のポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSSMManagedInstanceCore` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 3 月 15 日 17:22 UTC
- 編集日時: 2019 年 5 月 23 日 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
```

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSSMPatchAssociation

`AmazonSSMPatchAssociation` は、パッチアソシエーション操作用の子インスタンスへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSSMPatchAssociation` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 5 月 13 日 16:00 UTC
- 編集日時: 2020 年 5 月 13 日 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMPatchAssociation`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSSMReadOnlyAccess

`AmazonSSMReadOnlyAccess` は、Amazon SSM への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSSMReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 5 月 29 日 17:44 UTC
- 編集日時: 2015 年 5 月 29 日 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSSMServiceRolePolicy

AmazonSSMServiceRolePolicy は、Amazon SSM が管理または使用する AWS リソースへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 13 日 19:20 UTC
- 編集日時: 2022 年 9 月 14 日 19:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonSumerianFullAccess

AmazonSumerianFullAccess は、Amazon Sumerian へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSumerianFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 4 月 24 日 20:14 UTC
- 編集日時: 2018 年 4 月 24 日 20:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSumerianFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonTextractFullAccess

AmazonTextractFullAccess は、すべての Amazon Textract API へのアクセスを行う AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonTextractFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 28 日 19:07 UTC
- 編集日時: 2018 年 11 月 28 日 19:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTextractFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonTextractServiceRole

`AmazonTextractServiceRole` は、Textract がユーザーに代わって AWS サービスを呼び出すことを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonTextractServiceRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 11 月 28 日 19:12 UTC
- 編集日時: 2018 年 11 月 28 日 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:AmazonTextract*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonTimestreamConsoleFullAccess

`AmazonTimestreamConsoleFullAccess` は、AWS Management Console を使用して Amazon Timestream を管理するためのフルアクセスを提供する AWS マネージドポリシーです。このポリシーでは、特定の KMS オペレーションや、保存したクエリを管理する操作に対するアクセス許可も付与されることに注意してください。カスタマー管理型 CMK を使用している場合は、必要な追加のアクセス許可についてドキュメントを参照してください。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonTimestreamConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 9 月 30 日 21:47 UTC
- 編集日時: 2022 年 2 月 1 日 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonTimestreamFullAccess

AmazonTimestreamFullAccess は、Amazon Timestream へのフルアクセスを提供する AWS マネージドポリシーです。このポリシーでは、特定の KMS オペレーションへのアクセス許可も付与されることに注意してください。カスタマー管理型 CMK を使用している場合は、必要な追加のアクセス許可についてドキュメントを参照してください。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonTimestreamFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 9 月 30 日 21:47 UTC
- 編集日時: 2021 年 11 月 26 日 23:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonTimestreamInfluxDBFullAccess

AmazonTimestreamInfluxDBFullAccess は、Amazon Timestream InfluxDB インスタンスの作成、更新、削除、一覧表示、およびパラメータグループの作成と一覧表示を行うための完全な管理アクセスを提供する AWS マネージドポリシーです。必要な追加のアクセス許可については、「 ドキュメント」を参照してください。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonTimestreamInfluxDBFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時刻: 2024 年 3 月 14 日 22:53 UTC
- 編集日時： 2024 年 3 月 14 日 22:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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:::*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonTimestreamInfluxDBServiceRolePolicy

AmazonTimestreamInfluxDBServiceRolePolicy は、Amazon Timestream InfluxDB インスタンスの作成、更新、削除、一覧表示、およびパラメータグループの作成と一覧表示を行うための完全な管理アクセスを提供する AWS マネージドポリシーです。必要な追加のアクセス許可については、「 ドキュメント」を参照してください。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成時刻: 2024 年 3 月 14 日 18:53 UTC
- 編集日時： 2024 年 3 月 14 日 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
```

```
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonTimestreamReadOnlyAccess

AmazonTimestreamReadOnlyAccess は、Amazon Timestream への読み取り専用アクセスを提供する AWS マネージドポリシーです。ポリシーには、実行中のクエリをキャンセルするアクセス許可も付与されます。カスタマー管理型 CMK を使用している場合は、必要な追加のアクセス許可についてドキュメントを参照してください。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonTimestreamReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 9 月 30 日 21:47 UTC
- 編集日時: 2023 年 2 月 28 日 18:22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonTranscribeFullAccess

`AmazonTranscribeFullAccess` は、Amazon Transcribe の操作へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonTranscribeFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 4 月 4 日 16:06 UTC
- 編集日時: 2018 年 4 月 4 日 16:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*transcribe*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonTranscribeReadOnlyAccess

AmazonTranscribeReadOnlyAccess は、Amazon Transcribe の読み取り専用オペレーションへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonTranscribeReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 4 月 4 日 16:05 UTC
- 編集日時: 2018 年 4 月 4 日 16:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:Get*",
        "transcribe:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonVPCCrossAccountNetworkInterfaceOperations

AmazonVPCCrossAccountNetworkInterfaceOperations は、ネットワークインターフェイスを作成し、クロスアカウントリソースにアタッチするためのアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonVPCCrossAccountNetworkInterfaceOperations をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 7 月 18 日 20:47 UTC
- 編集日時: 2023 年 9 月 25 日 15:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonVPCFullAccess

`AmazonVPCFullAccess` は、経由で Amazon VPC へのフルアクセスを提供する AWS マネージドポリシーです AWS Management Console。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonVPCFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時： 2024 年 2 月 8 日 16:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

`AmazonVPCNetworkAccessAnalyzerFullAccessPolicy` は、AWS リソースの記述、Network Access Analyzer の実行、Network Insights Access Scope および Network Insights Access Scope Analysis のタグの作成または削除を行う AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonVPCNetworkAccessAnalyzerFullAccessPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 6 月 15 日 22:56 UTC
- 編集日時: 2023 年 11 月 3 日 19:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonVPCReachabilityAnalyzerFullAccessPolicy

`AmazonVPCReachabilityAnalyzerFullAccessPolicy` は、AWS リソースの記述、Reachability Analyzer の実行、Network Insights Path および Network Insights Analysis のタグの作成または削除を行う AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonVPCReachabilityAnalyzerFullAccessPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 6 月 14 日 20:12 UTC
- 編集日時: 2023 年 11 月 3 日 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerFullAccessPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

`AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` は、IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess というロールにアタッチされる AWS マネージドポリシーです。管理アカウントが Reachability Analyzer に対して信頼できるアクセスを有効にすると、このロールは組織のメンバーアカウントに展開されます。Reachability Analyzer コンソールを使用して組織全体のリソースを表示するためのアクセス許可を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 5 月 1 日 20:38 UTC
- 編集日時: 2023 年 5 月 1 日 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:Describe*",
        "network-firewall:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonVPCReadOnlyAccess

`AmazonVPCReadOnlyAccess` は、経由で Amazon VPC への読み取り専用アクセスを提供する AWS マネージドポリシーです AWS Management Console。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonVPCReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC

- 編集日時： 2024 年 2 月 8 日 17:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AmazonWorkDocsFullAccess

AmazonWorkDocsFullAccess は、AWS Management Console 経由で Amazon WorkDocs へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkDocsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 4 月 16 日 23:05 UTC
- 編集日時: 2020 年 4 月 16 日 23:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonWorkDocsReadOnlyAccess

AmazonWorkDocsReadOnlyAccess は、AWS Management Console 経由で Amazon WorkDocs への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkDocsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 1 月 8 日 23:49 UTC
- 編集日時: 2020 年 1 月 8 日 23:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonWorkMailEventsServiceRolePolicy

AmazonWorkMailEventsServiceRolePolicy は、Amazon WorkMail イベントが使用または管理する AWS のサービス およびリソースへのアクセスを可能にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 4 月 16 日 16:52 UTC
- 編集日時: 2019 年 4 月 16 日 16:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonWorkMailFullAccess

`AmazonWorkMailFullAccess` は、WorkMail、Directory Service、SES、EC2 へのフルアクセスと KMS メタデータへの読み取りアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonWorkMailFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC

- 編集日時: 2020 年 12 月 21 日 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonWorkMailMessageFlowFullAccess

AmazonWorkMailMessageFlowFullAccess は、WorkMail メッセージフロー API へのフルアクセスを実現するマネージドポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkMailMessageFlowFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 2 月 11 日 11:08 UTC
- 編集日時: 2021 年 2 月 11 日 11:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonWorkMailMessageFlowReadOnlyAccess

AmazonWorkMailMessageFlowReadOnlyAccess は、GetRawMessageContent API の WorkMail メッセージへの読み取り専用アクセス権限の AWS マネージドポリシー です

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkMailMessageFlowReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2021 年 1 月 28 日 12:40 UTC
- 編集日時: 2021 年 1 月 28 日 12:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonWorkMailReadOnlyAccess

`AmazonWorkMailReadOnlyAccess` は、WorkMail と SES への読み取り専用アクセスを提供するマネージドポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkMailReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2019 年 7 月 25 日 08:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
```

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonWorkSpacesAdmin

`AmazonWorkSpacesAdmin` は、AWS SDK と CLI 経由で Amazon WorkSpaces の管理アクションへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonWorkSpacesAdmin` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 9 月 22 日 22:21 UTC
- 編集日時: 2023 年 8 月 3 日 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonWorkSpacesApplicationManagerAdminAccess

AmazonWorkSpacesApplicationManagerAdminAccess は、Amazon WorkSpaces アプリケーションマネージャーでアプリケーションをパッケージ化するための管理者アクセスを提供するマネージドポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkSpacesApplicationManagerAdminAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 4 月 9 日 14:03 UTC
- 編集日時: 2015 年 4 月 9 日 14:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonWorkspacesPCAAccess

AmazonWorkspacesPCAAccess は、AWS アカウント の AWS Certificate Manager プライベート CA リソースへの完全な管理アクセスを提供し、証明書ベースの認証を可能にする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkspacesPCAAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 8 日 00:25 UTC
- 編集日時: 2022 年 11 月 8 日 00:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonWorkSpacesSelfServiceAccess

`AmazonWorkSpacesSelfServiceAccess` は、Amazon WorkSpaces バックエンドサービスにアクセスして WorkSpace セルフサービスアクションを実行できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonWorkSpacesSelfServiceAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2019 年 6 月 27 日 19:22 UTC
- 編集日時: 2019 年 6 月 27 日 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonWorkSpacesServiceAccess

AmazonWorkSpacesServiceAccess は、WorkSpace を起動するための AWS WorkSpaces サービスへのカスタマーアカウントアクセスを提供する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkSpacesServiceAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 6 月 27 日 19:19 UTC
- 編集日時: 2020 年 3 月 18 日 23:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonWorkSpacesWebReadOnly

`AmazonWorkSpacesWebReadOnly` は、AWS Management Console、SDK、および CLI 経由で Amazon WorkSpaces Web とその依存関係への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonWorkSpacesWebReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 30 日 14:20 UTC
- 編集日時: 2022 年 11 月 2 日 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonWorkSpacesWebServiceRolePolicy

AmazonWorkSpacesWebServiceRolePolicy は、Amazon WorkSpaces Web AWS のサービスが使用または管理するリソースへのアクセスを有効にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 30 日 13:15 UTC
- 編集日時: 2022 年 12 月 15 日 22:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
```

```
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonZocaloFullAccess

AmazonZocaloFullAccess は、Amazon Zocalo へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonZocaloFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonZocaloFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmazonZocaloReadOnlyAccess

AmazonZocaloReadOnlyAccess は、Amazon Zocalo への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonZocaloReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AmplifyBackendDeployFullAccess

AmplifyBackendDeployFullAccess は、AWS クラウド開発キットAWS (CDK) を介して Amplify バックエンドリソース (AWS AppSync、Amazon Cognito、Amazon S3、およびその他の関連サービス) をデプロイするためのフルアクセス許可を Amplify に提供する AWSマネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AmplifyBackendDeployFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 10 月 6 日 21:32 UTC
- 編集日時： 2024 年 1 月 2 日 21:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

APIGatewayServiceRolePolicy

APIGatewayServiceRolePolicy は、API ゲートウェイがお客様に代わって関連する AWS リソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 20 日 17:23 UTC
- 編集日時: 2021 年 7 月 12 日 22:24 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AppIntegrationsServiceLinkedRolePolicy

AppIntegrationsServiceLinkedRolePolicy は、AppIntegrations がユーザーに代わって AppFlow リソースを管理し、CloudWatch メトリクスデータを公開することを許可する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 9 月 30 日 19:42 UTC
- 編集日時: 2022 年 9 月 30 日 19:42 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ApplicationAutoScalingForAmazonAppStreamAccess

ApplicationAutoScalingForAmazonAppStreamAccess は、Amazon AppStream のアプリケーション自動スケーリングを有効にするポリシーとなる AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ApplicationAutoScalingForAmazonAppStreamAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 2 月 6 日 21:39 UTC
- 編集日時: 2017 年 2 月 6 日 21:39 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy は、AWS のサービス および、Application Service Continuous Export 機能によって使用または管理されているリソースへのアクセスを有効にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 8 月 9 日 20:22 UTC
- 編集日時: 2018 年 8 月 13 日 22:31 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AppRunnerNetworkingServiceRolePolicy

AppRunnerNetworkingServiceRolePolicy は、AWS AppRunner Networking がユーザーに代わって関連 AWS リソースを管理することを許可する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 1 月 12 日 21:02 UTC
- 編集日時: 2022 年 1 月 12 日 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AppRunnerServiceRolePolicy

AppRunnerServiceRolePolicy は、AWS AppRunner がユーザーに代わって関連 AWS リソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 5 月 14 日 19:15 UTC
- 編集日時: 2021 年 5 月 14 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AutoScalingConsoleFullAccess

AutoScalingConsoleFullAccess は、AWS Management Console 経由で自動スケーリングへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AutoScalingConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 1 月 12 日 19:43 UTC
- 編集日時: 2018 年 2 月 6 日 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
```

```
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AutoScalingConsoleReadOnlyAccess

`AutoScalingConsoleReadOnlyAccess` は、AWS Management Console 経由で自動スケーリングへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AutoScalingConsoleReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 1 月 12 日 19:48 UTC
- 編集日時: 2017 年 1 月 12 日 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AutoScalingFullAccess

`AutoScalingFullAccess` は、自動スケーリングへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AutoScalingFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 1 月 12 日 19:31 UTC
- 編集日時: 2018 年 2 月 6 日 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AutoScalingNotificationAccessRole

`AutoScalingNotificationAccessRole` は、AutoScaling 通知アクセスサービスロールのデフォルトポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AutoScalingNotificationAccessRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AutoScalingReadOnlyAccess

AutoScalingReadOnlyAccess は、自動スケーリングへ読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AutoScalingReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 1 月 12 日 19:39 UTC
- 編集日時: 2017 年 1 月 12 日 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AutoScalingServiceRolePolicy

AutoScalingServiceRolePolicy は、Auto Scaling が使用または管理する AWS のサービス およびリソースへのアクセスを有効にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 1 月 8 日 23:10 UTC
- 編集日時： 2024 年 2 月 29 日 17:48 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWS_ConfigRole

AWS_ConfigRole は、 AWS Config サービスロールのデフォルトポリシーである AWS マネージドポリシーです。 AWS Config が AWS リソースの変更を追跡するために必要なアクセス許可を提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに AWS_ConfigRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2020 年 9 月 15 日 20:30 UTC
- 編集日時： 2024 年 2 月 22 日 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWS_ConfigRole`

ポリシーのバージョン

ポリシーのバージョン: v30 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSAccountActivityAccess

`AWSAccountActivityAccess` は、ユーザーが [アカウント活動] ページにアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSAccountActivityAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2023 年 3 月 7 日 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountActivityAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAccountManagementFullAccess

AWSAccountManagementFullAccess は、AWS アカウント管理へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAccountManagementFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 9 月 30 日 23:20 UTC
- 編集日時: 2021 年 9 月 30 日 23:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountManagementFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAccountManagementReadOnlyAccess

AWSAccountManagementReadOnlyAccess は、AWS アカウント管理への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAccountManagementReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 9 月 30 日 23:29 UTC
- 編集日時: 2021 年 9 月 30 日 23:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAccountUsageReportAccess

AWSAccountUsageReportAccess は、[アカウント使用状況レポート] ページへのアクセスをユーザーに許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAccountUsageReportAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountUsageReportAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewUsage"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAgentlessDiscoveryService

`AWSAgentlessDiscoveryService` は、Discovery Agentless コネクタが AWS Application Discovery サービスに登録するためのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSAgentlessDiscoveryService` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 8 月 2 日 01:35 UTC
- 編集日時: 2020 年 2 月 24 日 23:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAppFabricFullAccess

AWSAppFabricFullAccess は、AWS AppFabric サービスへのフルアクセスと S3、Kinesis、KMS などの依存サービスへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppFabricFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 6 月 27 日 19:51 UTC
- 編集日時: 2023 年 6 月 27 日 19:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppFabricFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAppFabricReadOnlyAccess

`AWSAppFabricReadOnlyAccess` は、AWS AppFabric への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSAppFabricReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 6 月 27 日 19:52 UTC
- 編集日時: 2023 年 6 月 27 日 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAppFabricServiceRolePolicy

AWSAppFabricServiceRolePolicy は、ユーザーに代わって AppFabric が AWS リソースにアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 6 月 26 日 21:07 UTC

- 編集日時: 2023 年 6 月 26 日 21:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationAutoscalingAppStreamFleetPolicy

AWSApplicationAutoscalingAppStreamFleetPolicy は、AppStream と CloudWatch にアクセスするためのアクセス許可をアプリケーションの自動スケーリングに付与する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 20 日 19:04 UTC

- 編集日時: 2017 年 10 月 20 日 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationAutoscalingCassandraTablePolicy

AWSApplicationAutoscalingCassandraTablePolicy は、Cassandra と CloudWatch にアクセスするためのアクセス許可をアプリケーションの自動スケーリングに付与する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 3 月 18 日 22:49 UTC
- 編集日時: 2020 年 3 月 18 日 22:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationAutoscalingComprehendEndpointPolicy

AWSApplicationAutoscalingComprehendEndpointPolicy は、Comprehend と CloudWatch にアクセスするためのアクセス権限をアプリケーションの自動スケーリングに付与する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 14 日 18:39 UTC
- 編集日時: 2019 年 11 月 14 日 18:39 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationAutoScalingCustomResourcePolicy

AWSApplicationAutoScalingCustomResourcePolicy は、APIGateway と CloudWatch にアクセスしてカスタムリソーススケーリングを行うためのアクセス許可をアプリケーションの自動スケーリングに付与する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 6 月 4 日 23:22 UTC
- 編集日時: 2018 年 6 月 4 日 23:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
```

```
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationAutoscalingDynamoDBTablePolicy

AWSApplicationAutoscalingDynamoDBTablePolicy は、DynamoDB と CloudWatch にアクセスするためのアクセス許可をアプリケーションの自動スケーリングに付与する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 20 日 21:34 UTC
- 編集日時: 2017 年 10 月 20 日 21:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy は、EC2 スポットフリートと CloudWatch にアクセスするためのアクセス権限をアプリケーションの自動スケーリングに付与する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 25 日 18:23 UTC
- 編集日時: 2017 年 10 月 25 日 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationAutoscalingECSServicePolicy

AWSApplicationAutoscalingECSServicePolicy は、EC2 コンテナサービスと CloudWatch にアクセスするためのアクセス権限をアプリケーションの自動スケーリングに付与する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 25 日 23:53 UTC
- 編集日時: 2017 年 10 月 25 日 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationAutoscalingElastiCacheRGPolicy

AWSApplicationAutoscalingElastiCacheRGPolicy は、Amazon ElastiCache と Amazon CloudWatch にアクセスするためのアクセス許可をアプリケーションの自動スケーリングに付与する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 8 月 17 日 23:41 UTC

- 編集日時: 2021 年 8 月 17 日 23:41 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
```

```
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationAutoscalingEMRInstanceGroupPolicy

AWSApplicationAutoscalingEMRInstanceGroupPolicy は、Elastic Map Reduce と CloudWatch にアクセスするためのアクセス許可をアプリケーションの自動スケーリングに付与する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 26 日 00:57 UTC
- 編集日時: 2017 年 10 月 26 日 00:57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationAutoscalingKafkaClusterPolicy

AWSApplicationAutoscalingKafkaClusterPolicy は、Apache Kafka と CloudWatch のマネージドストリーミングにアクセスするためのアクセス許可をアプリケーションの自動スケーリングに付与する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2020 年 8 月 24 日 18:36 UTC
- 編集日時: 2020 年 8 月 24 日 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationAutoscalingLambdaConcurrencyPolicy

AWSApplicationAutoscalingLambdaConcurrencyPolicy は、Lambda と CloudWatch にアクセスするためのアクセス許可をアプリケーションの自動スケーリングに付与する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 10 月 21 日 20:04 UTC
- 編集日時: 2019 年 10 月 21 日 20:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationAutoscalingNeptuneClusterPolicy

AWSApplicationAutoscalingNeptuneClusterPolicy は、Amazon Neptune と Amazon CloudWatch にアクセスするためのアクセス許可をアプリケーションの自動スケーリングに付与する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 9 月 2 日 21:14 UTC
- 編集日時: 2021 年 9 月 2 日 21:14 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationAutoscalingRDSClusterPolicy

AWSApplicationAutoscalingRDSClusterPolicy は、RDS と CloudWatch にアクセスするためのアクセス許可をアプリケーションの自動スケーリングに付与する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 17 日 17:46 UTC
- 編集日時: 2018 年 8 月 7 日 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationAutoscalingSageMakerEndpointPolicy

AWSApplicationAutoscalingSageMakerEndpointPolicyは、Application Auto Scaling AWS SageMaker CloudWatchにおよびへのアクセス権限を付与する管理ポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 2 月 6 日 19:58 UTC
- 編集日時: 2023 年 11 月 13 日 18:52 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
```

```
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationDiscoveryAgentAccess

AWSApplicationDiscoveryAgentAccess は、検出エージェントが AWS Application Discovery Service に登録するためのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationDiscoveryAgentAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 5 月 11 日 21:38 UTC
- 編集日時: 2020 年 2 月 24 日 22:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationDiscoveryAgentlessCollectorAccess

`AWSApplicationDiscoveryAgentlessCollectorAccess` は、Application Discovery Service エージェントレスコレクターが自動更新、登録、および Application Discovery Service と通信できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSApplicationDiscoveryAgentlessCollectorAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2022 年 8 月 16 日 21:00 UTC
- 編集日時: 2022 年 8 月 16 日 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentlessCollectorAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationDiscoveryServiceFullAccess

AWSApplicationDiscoveryServiceFullAccess は、AWS Application Discovery Service によって管理される設定項目を表示し、タグ付けするためのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationDiscoveryServiceFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 5 月 11 日 21:30 UTC

- 編集日時: 2019 年 6 月 19 日 21:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationMigrationAgentInstallationPolicy

AWSApplicationMigrationAgentInstallationPolicy は、外部サーバーを AWS へ移行するために AWS アプリケーション移行サービス (MGN) とともに使用される AWS レプリケーションエージェントをインストールできるようにする AWS マネージドポリシーです。このポリシー

は、AWS レプリケーションエージェントのインストール時に指定した認証情報を持つ IAM ユーザーまたはロールにアタッチします。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationAgentInstallationPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 6 月 19 日 07:51 UTC
- 編集日時: 2022 年 9 月 20 日 11:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationMigrationAgentPolicy

AWSApplicationMigrationAgentPolicy は、外部サーバーを AWS へ移行するために AWS アプリケーション移行サービス (MGN) と併用される AWS レプリケーションエージェントのインストールと使用を許可する AWS マネージドポリシーです。このポリシーは、AWS レプリケーションエージェントのインストール時に指定した認証情報を持つ IAM ユーザーまたはロールにアタッチします。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationAgentPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 4 月 7 日 07:00 UTC
- 編集日時: 2022 年 9 月 20 日 11:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationMigrationAgentPolicy_v2

AWSApplicationMigrationAgentPolicy_v2 は、AWS アプリケーション移行サービス (MGN) と併用される AWS レプリケーションエージェントを使用して、外部サーバーを AWS へ移行することを可能にする AWS マネージドポリシーです。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationAgentPolicy_v2 をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 6 月 6 日 14:14 UTC
- 編集日時: 2022 年 6 月 6 日 14:14 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationMigrationConversionServerPolicy

AWSApplicationMigrationConversionServerPolicy は、アプリケーション移行サービスによって起動される EC2 インスタンスであるアプリケーション移行サービス (MGN) 変換サーバーが MGN サービスと通信できるようにする AWS マネージドポリシーです。このポリシーの付いた IAM ロールは MGN によって (EC2 インスタンスプロファイルとして) MGN 変換サーバーにアタッチされ、MGN は必要に応じて自動的に起動および終了します。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。MGN 変換サーバーは、ユーザーが MGN コンソール、CLI、または API を使用してテストインスタンスまたはカットオーバーインスタンスを起動することを選択したときに、アプリケーション移行サービスによって使用されます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationConversionServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 4 月 7 日 06:48 UTC
- 編集日時: 2021 年 4 月 7 日 06:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationMigrationEC2Access

AWSApplicationMigrationEC2Access は、アプリケーション移行サービス (MGN) を使用して移行したサーバーを EC2 インスタンスとして起動するために必要な Amazon EC2 オペレーションを提供する AWS マネージドポリシーです。このポリシーを IAM ユーザーまたはロールにアタッチします。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationEC2Access をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 4 月 7 日 07:05 UTC
- 編集日時: 2023 年 2 月 6 日 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
```

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationMigrationFullAccess

AWSApplicationMigrationFullAccess は、AWS アプリケーション移行サービス (MGN) のすべてのパブリック API に対するアクセス許可と、KMS キー情報を読み取る権限を付与する AWS マネージドポリシーです。このポリシーを IAM ユーザーまたはロールにアタッチします。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 4 月 7 日 06:56 UTC
- 編集日時: 2023 年 4 月 20 日 17:28 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationMigrationMGHAccess

AWSApplicationMigrationMGHAccess は、AWS Application Migration Service (MGN) が MGN を使用して AWS Migration Hub (MGH) に移行中のサーバーの進捗に関するメタデータの送信を可能にする AWS マネージドポリシーです。MGN は、このポリシーがアタッチされた IAM ロールを自動的に作成し、このロールを引き受けます。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationMGHAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 4 月 7 日 07:10 UTC
- 編集日時: 2021 年 4 月 7 日 07:10 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationMigrationReadOnlyAccess

`AWSApplicationMigrationReadOnlyAccess` は、Application Migration Service (MGN) のすべての読み取り専用パブリック API だけでなく、MGN コンソールを読み取り専用で完全に使用するために必要な、他の AWS サービスの読み取り専用 API にもアクセス許可を付与する AWS マネージドポリシーです。このポリシーを IAM ユーザーまたはロールにアタッチします。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 4 月 7 日 07:15 UTC
- 編集日時: 2023 年 3 月 20 日 08:58 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationMigrationReplicationServerPolicy

AWSApplicationMigrationReplicationServerPolicy は、Application Migration Service (MGN) レプリケーション サーバー (Application Migration Service によって起動される EC2 インスタンス) が MGN サービスと通信し、AWS アカウント のサーバーに EBS スナップショットを作成できるようにする AWS マネージドポリシーです。このポリシーを含む IAM ロールは、アプリケー

ション移行サービスによって MGN レプリケーションサーバーに (EC2 インスタンスプロファイルとして) アタッチされます。MGN レプリケーションサーバーは、必要に応じて MGN によって自動的に起動および終了されます。MGN レプリケーションサーバーは、MGN を使用して管理される AWS への移行プロセスの一環として、外部サーバーからのデータ複製を容易にするために使用されます。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSApplicationMigrationReplicationServerPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 4 月 7 日 07:21 UTC
- 編集日時: 2021 年 4 月 7 日 07:21 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationMigrationServiceEc2InstancePolicy

AWSApplicationMigrationServiceEc2InstancePolicy は、AWS アプリケーション移行サービス (AWS MGN) が EC2 上で稼働するソースサーバー (クロスリージョンまたは Cross-AZ) を移行するために使用する AWS レプリケーションエージェントのインストールと使用を許可する AWS マネージドポリシーです。このポリシーを含む IAM ロールは、EC2 インスタンスに (EC2 インスタンスプロファイルとして) アタッチする必要があります。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationServiceEc2InstancePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 8 月 22 日 13:19 UTC

- 編集日時： 2024 年 1 月 3 日 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationMigrationServiceRolePolicy

AWSApplicationMigrationServiceRolePolicy は、AWS アプリケーション移行サービスがユーザーに代わって AWS リソースを作成および管理することを許可する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 4 月 7 日 06:43 UTC
- 編集日時: 2023 年 6 月 20 日 09:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationMigrationSSMAccess

AWSApplicationMigrationSSMAccess は、アプリケーション移行サービス (MGN) を使用して移行後のカスタムコマンド SSM ドキュメントを実行するために必要な Amazon SSM オペレーションへのアクセス権を提供する AWS マネージドポリシーです。このポリシーを IAM ユーザーまたはロールにアタッチします。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationSSMAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2022 年 11 月 27 日 9:29 UTC
- 編集日時: 2023 年 3 月 20 日 10:57 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSApplicationMigrationVCenterClientPolicy

AWSApplicationMigrationVCenterClientPolicy は、外部サーバーを AWS に移行するために AWS アプリケーション移行サービス (MGN) とともに使用される AWS vCenter Client のインストールと使用を許可する AWS マネージドポリシーです。AWS vCenter Client のインストール時に指定した認証情報を持つ IAM ユーザーまたはロールにこのポリシーをアタッチします。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationVCenterClientPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 8 日 12:53 UTC
- 編集日時: 2021 年 11 月 8 日 12:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAppMeshEnvoyAccess

AWSAppMeshEnvoyAccess は、仮想ノード構成にアクセスするための App Mesh Envoy ポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppMeshEnvoyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 7 月 3 日 21:29 UTC
- 編集日時: 2019 年 7 月 3 日 21:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAppMeshFullAccess

AWSAppMeshFullAccess は、AWS App Mesh API と管理コンソールへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppMeshFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 4 月 16 日 17:50 UTC
- 編集日時: 2021 年 1 月 7 日 19:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAppMeshPreviewEnvoyAccess

AWSAppMeshPreviewEnvoyAccess は、仮想ノード構成にアクセスするための App Mesh Preview Envoy ポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppMeshPreviewEnvoyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 8 月 5 日 23:32 UTC
- 編集日時: 2019 年 8 月 5 日 23:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAppMeshPreviewServiceRolePolicy

AWSAppMeshPreviewServiceRolePolicy は、AWS App Mesh が使用または管理する AWS のサービス およびリソースへのアクセスを有効にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 19 日 19:07 UTC
- 編集日時: 2019 年 8 月 21 日 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAppMeshReadOnly

AWSAppMeshReadOnly は、AWS App Mesh API と管理コンソールへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppMeshReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 4 月 16 日 17:51 UTC
- 編集日時: 2021 年 1 月 7 日 19:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshReadOnly

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAppMeshServiceRolePolicy

AWSAppMeshServiceRolePolicy は、AWS AppMesh が使用または管理する AWS のサービス およびリソースへのアクセスを有効にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 3 日 18:30 UTC
- 編集日時: 2023 年 10 月 10 日 16:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAppRunnerFullAccess

AWSAppRunnerFullAccess は、App Runner のすべてのアクションにアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppRunnerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 1 月 11 日 04:02 UTC
- 編集日時: 2022 年 1 月 11 日 04:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppRunnerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAppRunnerReadOnlyAccess

AWSAppRunnerReadOnlyAccess は、App Runner リソースの詳細をリストおよび表示するアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppRunnerReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 2 月 24 日 21:24 UTC
- 編集日時: 2022 年 2 月 24 日 21:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apprunner:List*",
        "apprunner:Describe*"
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAppRunnerServicePolicyForECRAccess

AWSAppRunnerServicePolicyForECRAccess は、お客様のアカウントの Amazon ECR リソースへの読み取り権限を付与する AWS App Runner サービスポリシーである AWS マネージドポリシー です。App Runner サービスを作成または更新するときに App Runner に渡されるロールで使用してください。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppRunnerServicePolicyForECRAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 5 月 14 日 19:17 UTC
- 編集日時: 2021 年 5 月 14 日 19:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAppSyncAdministrator

`AWSAppSyncAdministrator` は、AppSync サービスへの管理アクセスを提供する AWS マネージドポリシーです。ただし、コンソールからアクセスするには不十分です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSAppSyncAdministrator` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 3 月 20 日 21:20 UTC
- 編集日時: 2019 年 11 月 4 日 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncAdministrator`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAppSyncInvokeFullAccess

AWSAppSyncInvokeFullAccess は、AppSync サービスへの完全な呼び出しアクセスを、コンソール経由でも単独でも提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppSyncInvokeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 3 月 20 日 21:21 UTC
- 編集日時: 2018 年 3 月 20 日 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAppSyncPushToCloudWatchLogs

AWSAppSyncPushToCloudWatchLogs は、AppSync がユーザーの CloudWatch アカウントにログをプッシュすることを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppSyncPushToCloudWatchLogs をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 4 月 9 日 19:38 UTC
- 編集日時: 2018 年 4 月 9 日 19:38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAppSyncSchemaAuthor

AWSAppSyncSchemaAuthor は、スキーマの作成、更新、クエリを行うためのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppSyncSchemaAuthor をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 3 月 20 日 21:21 UTC
- 編集日時: 2023 年 2 月 1 日 18:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAppSyncServiceRolePolicy

AWSAppSyncServiceRolePolicy は、AWS AppSync が使用または管理するサービスとリソースへのアクセスを有効にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 1 月 21 日 19:56 UTC
- 編集日時: 2020 年 1 月 21 日 19:56 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSArtifactAccountSync

AWSArtifactAccountSync は、AWS 組織内の操作への AWS Artifact の読み取り専用アクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSArtifactAccountSync をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 4 月 10 日 23:04 UTC
- 編集日時: 2018 年 4 月 10 日 23:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSArtifactReportsReadOnlyAccess

`AWSArtifactReportsReadOnlyAccess` は、 AWS Artifact サービスレポートへの読み取り専用アクセスを提供する AWSマネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSArtifactReportsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時刻: 2024 年 1 月 2 日 22:42 UTC
- 編集日時： 2024 年 1 月 2 日 22:42 UTC
- ARN: arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSArtifactServiceRolePolicy

AWSArtifactServiceRolePolicy は、AWS Artifact が AWS Organizations サービス経由で組織に関する情報を収集することを許可する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 8 月 21 日 20:27 UTC
- 編集日時: 2023 年 8 月 21 日 20:27 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAuditManagerAdministratorAccess

AWSAuditManagerAdministratorAccess は、AWS Audit Manager の有効化または無効化、設定の更新、評価、統制、フレームワークの管理を行うための管理アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAuditManagerAdministratorAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 11 日 20:02 UTC
- 編集日時: 2022 年 4 月 30 日 00:02 UTC

- ARN: arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAuditManagerServiceRolePolicy

AWSAuditManagerServiceRolePolicy は、AWS Audit Manager が使用または管理する AWS のサービスおよびリソースへのアクセスを有効にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 8 日 15:12 UTC
- 編集時間:2023 年 12 月 6 日 20:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "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"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSAutoScalingPlansEC2AutoScalingPolicy

AWSAutoScalingPlansEC2AutoScalingPolicy は、AWS Auto Scaling にアクセス許可を付与して、定期的に容量を予測し、スケーリングプラン内の Auto Scaling グループのスケジュールされたスケーリングアクションを生成する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 8 月 23 日 22:46 UTC
- 編集日時: 2018 年 8 月 23 日 22:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBackupAuditAccess

AWSBackupAuditAccess は、AWS Backup リソースとアクティビティに対する期待値を定義したコントロールとフレームワークを作成し、AWS Backup リソースとアクティビティを定義したコントロールとフレームワークに照らして監査する権限をユーザーに付与する AWS マネージドポリシーです。このポリシーは、ユーザーの期待を記述するために AWS Config や同様のサービスへの権

限を与え、監査を実行します。このポリシーは、S3 および同様のサービスに監査レポートを配信するアクセス権限も付与し、ユーザーは監査レポートを見つけて開くことができます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupAuditAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 8 月 24 日 01:02 UTC
- 編集日時: 2023 年 4 月 10 日 21:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupAuditAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:::*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBackupDataTransferAccess

AWSBackupDataTransferAccess は、AWS Backint エージェントが AWS Backup ストレージプレーンとのバックアップデータ転送を完了できるようにする AWS マネージドポリシーです。このポリシーを Backint エージェントで SAP HANA を実行している EC2 インスタンスが引き受けるロールにアタッチします。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupDataTransferAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 10 日 22:48 UTC
- 編集日時: 2022 年 11 月 10 日 22:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupDataTransferAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBackupFullAccess

AWSBackupFullAccess は、Backup 管理者を対象としており、バックアップ計画の作成や編集、バックアッププランへの AWS リソースの割り当て、バックアップの削除、バックアップの復元など、AWS バックアップのオペレーションにフルアクセスを可能にする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 11 月 18 日 22:21 UTC
- 編集時間:2023 年 11 月 27 日 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupFullAccess

ポリシーのバージョン

ポリシーのバージョン: v17 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync は、ユーザーに代わって仮想マシンのメタデータを同期する AWS BackupGateway 権限を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 12 月 15 日 19:43 UTC
- 編集日時: 2022 年 12 月 15 日 19:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBackupOperatorAccess

AWSBackupOperatorAccess は、AWS バックアッププランへのリソースの割り当て、オンデマンドバックアップの作成、バックアップの復元を行うアクセス許可をユーザーに付与する AWS マネージドポリシーです。このポリシーは、ユーザーがバックアッププランを作成、または編集したり、スケジュールされたバックアップを作成後に削除したりするためのアクセス許可は持っていません。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupOperatorAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 11 月 18 日 22:23 UTC
- 編集日時: 2023 年 9 月 6 日 20:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupOperatorAccess

ポリシーのバージョン

ポリシーのバージョン: v15 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBackupOrganizationAdminAccess

AWSBackupOrganizationAdminAccess は、クロスアカウントバックアップ管理を使用して組織のバックアップを管理するバックアップ管理者を対象とする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupOrganizationAdminAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 6 月 24 日 16:23 UTC
- 編集日時: 2022 年 11 月 18 日 18:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBackupRestoreAccessForSAPHANA

AWSBackupRestoreAccessForSAPHANA は、Amazon EC2 で SAP HANA のバックアップを復元するための AWS バックアップのアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupRestoreAccessForSAPHANA をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 10 日 22:43 UTC
- 編集日時: 2022 年 11 月 10 日 22:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*:*:*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBackupServiceLinkedRolePolicyForBackup

AWSBackupServiceLinkedRolePolicyForBackup は、ユーザーに代わって AWS サービス全体で AWS バックアップを作成するためのバックアップのアクセス許可を付与する、AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 6 月 2 日 23:08 UTC
- 編集時間:2023 年 12 月 15 日 22:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

ポリシーのバージョン

ポリシーのバージョン: v15 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
```

```
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBackupServiceLinkedRolePolicyForBackupTest

AWSBackupServiceLinkedRolePolicyForBackupTest は、ユーザーに代わって AWS サービス全体で AWS バックアップを作成するためのバックアップのアクセス許可を付与する、AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 5 月 12 日 17:37 UTC
- 編集日時: 2020 年 5 月 12 日 17:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBackupServiceRolePolicyForBackup

AWSBackupServiceRolePolicyForBackup は、ユーザーに代わって AWS サービス全体で AWS バックアップを作成するためのバックアップのアクセス許可を付与する、AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupServiceRolePolicyForBackup をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 1 月 10 日 21:01 UTC
- 編集時間:2023 年 12 月 15 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup

ポリシーのバージョン

ポリシーのバージョン: v18 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*:*:*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBackupServiceRolePolicyForRestores

AWSBackupServiceRolePolicyForRestores は、ユーザーに代わって AWS サービス間で復元を実行する AWS バックアップの権限を提供する AWS マネージドポリシーです。このポリシーには、復元プロセスの一部である EBS ボリューム、RDS インスタンス、EFS AWS ファイルシステムなどのリソースを作成および削除するアクセス許可が含まれています。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupServiceRolePolicyForRestores をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 1 月 12 日 00:23 UTC
- 編集時間:2023 年 12 月 15 日 22:05 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores

ポリシーのバージョン

ポリシーのバージョン: v20 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBackupServiceRolePolicyForS3Backup

AWSBackupServiceRolePolicyForS3Backup は、AWS バックアップが任意の S3 バケットのデータをバックアップするために必要なアクセス許可を含む AWS マネージドポリシーです。これには、すべての S3 オブジェクトへの読み取りアクセスと、すべての KMS キーに対する復号化アクセスが含まれます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupServiceRolePolicyForS3Backup をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 2 月 18 日 17:40 UTC
- 編集日時: 2022 年 9 月 1 日 16:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBackupServiceRolePolicyForS3Restore

AWSBackupServiceRolePolicyForS3Restore は、AWS バックアップが S3 Backup をバケットに復元するために必要なアクセス許可を含む AWS マネージドポリシーです。これには、すべての S3 バケットへの読み取り/書き込み権限、およびすべての KMS キーの GenerateDataKey と DescribeKey の生成権限が含まれます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupServiceRolePolicyForS3Restore をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 2 月 18 日 17:39 UTC
- 編集日時: 2023 年 2 月 7 日 00:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBatchFullAccess

`AWSBatchFullAccess` は、AWS Batch リソースへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSBatchFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 12 月 6 日 19:35 UTC
- 編集日時: 2022 年 10 月 24 日 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBatchFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBatchServiceEventTargetRole

AWSBatchServiceEventTargetRole は、AWS バッチジョブ送信用の CloudWatch イベントターゲットを有効にする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBatchServiceEventTargetRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 2 月 28 日 22:31 UTC
- 編集日時: 2018 年 2 月 28 日 22:31 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBatchServiceRole

`AWSBatchServiceRole` は、EC2、自動スケーリング、EC2 コンテナサービス、Cloudwatch Logs AWS などの関連サービスへのアクセスを許可する Batch サービスロール用の AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBatchServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 12 月 6 日 19:36 UTC
- 編集時間:2023 年 12 月 5 日 18:49 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole

ポリシーのバージョン

ポリシーのバージョン: v13 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBillingConductorFullAccess

`AWSBillingConductorFullAccess` は、AWSBillingConductorFullAccess マネージドポリシーを使用して AWS Billing Conductor (ABC) コンソールと API への完全なアクセスを許可する AWS マネージドポリシーです。このポリシーにより、ユーザーは ABC リソースを一覧表示、作成、削除できます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBillingConductorFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 4 月 13 日 18:02 UTC
- 編集日時: 2022 年 4 月 13 日 18:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSBillingConductorFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBillingConductorReadOnlyAccess

AWSBillingConductorReadOnlyAccess は、AWSBillingConductorReadOnlyAccess マネージドポリシーを使用して AWS Billing Conductor (ABC) コンソールと API への読み取り専用アクセスを許可する AWS マネージドポリシーです。このポリシーは、すべての ABC リソースを取得して一覧表示するアクセス許可を付与します。リソースを作成または削除したりする機能は含まれません。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBillingConductorReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 4 月 13 日 18:02 UTC
- 編集日時: 2022 年 4 月 13 日 18:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:List*",
        "organizations:ListAccounts",
        "pricing:DescribeServices"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBillingReadOnlyAccess

AWSBillingReadOnlyAccess は、ユーザーが請求コンソールで請求書を閲覧できるようにするAWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBillingReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 8 月 27 日 20:08 UTC
- 編集日時： 2024 年 1 月 17 日 18:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

`AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM` は、AWS リソースを制御するアクセス許可を付与する AWS マネージドポリシーです。例えば、AWS Systems Manager (SSM) スクリプトを実行することで、Amazon EC2 または Amazon RDS インスタンスを起動および停止します。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 5 月 25 日 19:03 UTC
- 編集日時: 2022 年 5 月 25 日 19:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBudgetsActionsWithAWSResourceControlAccess

`AWSBudgetsActionsWithAWSResourceControlAccess` は、Budgets アクションを使用して AWS Management Console 経由で実行中の AWS リソースの状態を制御するなど、AWS Budgets アクションへの完全なアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSBudgetsActionsWithAWSResourceControlAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 10 月 15 日 17:19 UTC
- 編集日時: 2020 年 10 月 15 日 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBudgetsReadOnlyAccess

`AWSBudgetsReadOnlyAccess` は、AWS Management Console 経由で AWS Budgets Console への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBudgetsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 10 月 15 日 17:18 UTC
- 編集日時: 2020 年 10 月 15 日 17:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBugBustFullAccess

AWSBugBustFullAccess は、IAM ポリシーであり、AWS BugBust コンソールへのフルアクセスをユーザーに付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBugBustFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 6 月 24 日 07:03 UTC
- 編集日時: 2021 年 7 月 22 日 20:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSBugBustFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBugBustPlayerAccess

AWSBugBustPlayerAccess は、IAM ポリシーでありは、AWS BugBust イベントに参加するためのアクセス許可をユーザーに付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBugBustPlayerAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 6 月 24 日 07:15 UTC
- 編集日時: 2021 年 6 月 24 日 07:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSBugBustPlayerAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSBugBustServiceRolePolicy

AWSBugBustServiceRolePolicy は、ユーザーに代わってリソースにアクセスする権限を AWS BugBust に付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 6 月 24 日 06:59 UTC
- 編集日時: 2021 年 6 月 24 日 06:59 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCertificateManagerFullAccess

`AWSCertificateManagerFullAccess` は、AWS Certificate Manager (ACM) へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCertificateManagerFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 1 月 21 日 17:02 UTC
- 編集日時: 2020 年 8 月 17 日 22:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCertificateManagerPrivateCAAuditor

AWSCertificateManagerPrivateCAAuditor は、AWS Certificate Manager のプライベート認証局への監査人アクセスを提供する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCertificateManagerPrivateCAAuditor をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 10 月 23 日 16:51 UTC
- 編集日時: 2020 年 8 月 17 日 22:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCertificateManagerPrivateCAFullAccess

`AWSCertificateManagerPrivateCAFullAccess` は、AWS Certificate Manager のプライベート認証局へのフルアクセスを提供する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCertificateManagerPrivateCAFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 10 月 23 日 16:54 UTC

- 編集日時: 2018 年 10 月 23 日 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCertificateManagerPrivateCAPrivilegedUser

`AWSCertificateManagerPrivateCAPrivilegedUser` は、特権証明書ユーザーに AWS Certificate Manager プライベート認証局へのアクセスを提供する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCertificateManagerPrivateCAPrivilegedUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 6 月 20 日 17:43 UTC
- 編集日時: 2019 年 6 月 20 日 17:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCertificateManagerPrivateCAReadOnly

AWSCertificateManagerPrivateCAReadOnly は、AWS Certificate Manager のプライベート認証局への読み取り専用アクセスを提供する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCertificateManagerPrivateCAReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 10 月 23 日 16:57 UTC
- 編集日時: 2020 年 8 月 17 日 22:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
  }
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCertificateManagerPrivateCAUser

`AWSCertificateManagerPrivateCAUser` は、証明書ユーザーに AWS Certificate Manager プライベート認証局へのアクセスを提供する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCertificateManagerPrivateCAUser` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 10 月 23 日 16:53 UTC
- 編集日時: 2019 年 6 月 20 日 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCertificateManagerReadOnly

`AWSCertificateManagerReadOnly` は、AWS Certificate Manager (ACM) への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCertificateManagerReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 1 月 21 日 17:07 UTC
- 編集日時: 2021 年 3 月 15 日 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:GetCertificate",
      "acm:ListTagsForCertificate",
      "acm:GetAccountConfiguration"
    ],
    "Resource" : "*"
  }
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSChatbotServiceLinkedRolePolicy

`AWSChatbotServiceLinkedRolePolicy` は、AWS Chatbot が使用するサービスリンクロールである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 18 日 16:39 UTC
- 編集日時: 2019 年 11 月 18 日 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCleanRoomsFullAccess

AWSCleanRoomsFullAccess は、 AWS クリーンルームリソースへのフルアクセスと、関連するへのアクセスを許可する AWS マネージドポリシーです AWS のサービス。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCleanRoomsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 1 月 12 日 16:10 UTC
- 編集日時： 2024 年 3 月 21 日 15:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSCleanRoomsFullAccessNoQuerying

AWSCleanRoomsFullAccessNoQuerying は、AWS クリーンルームリソースへのフルアクセス (コラボレーションでのクエリを除く) および関連する AWS のサービス リソースへのアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCleanRoomsFullAccessNoQuerying をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 1 月 12 日 16:12 UTC
- 編集日時: 2023 年 7 月 31 日 20:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCleanRoomsMLFullAccess

AWSCleanRoomsMLFullAccessは、AWSAWSクリーンルームのMLリソースへのフルアクセスと関連リソースへのアクセスを許可する管理ポリシーですAWS のサービス。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCleanRoomsMLFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時間:2023 年 11 月 29 日 21:02 UTC
- 編集時間:2023 年 11 月 29 日 21:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCleanRoomsMLReadOnlyAccess

AWSCleanRoomsMLReadOnlyAccessは、Clean Room ML AWSAWSAWSリソースへの読み取り専用アクセスと関連するクリーンルームリソースへの読み取り専用アクセスを許可する管理ポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCleanRoomsMLReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時間:2023 年 11 月 29 日 20:55 UTC
- 編集時間:2023 年 11 月 29 日 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
```

```
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCleanRoomsReadOnlyAccess

`AWSCleanRoomsReadOnlyAccess` は、AWSクリーンルームリソースへの読み取り専用アクセスと、関連する AWS Glue および Amazon CloudWatch Logs リソースへの読み取り専用アクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCleanRoomsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 1 月 12 日 16:10 UTC
- 編集日時: 2023 年 1 月 12 日 16:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloud9Administrator

`AWSCloud9Administrator` は、AWS Cloud9 への管理者アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloud9Administrator` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 30 日 16:17 UTC
- 編集日時: 2023 年 10 月 11 日 12:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9Administrator`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloud9EnvironmentMember

`AWSCloud9EnvironmentMember` は、AWS Cloud9 の共有開発環境に招待される機能を提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloud9EnvironmentMember` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 30 日 16:18 UTC
- 編集日時: 2023 年 10 月 11 日 12:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloud9ServiceRolePolicy

AWSCloud9ServiceRolePolicy は、AWS Cloud9 のサービスリンクロールポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 30 日 13:44 UTC
- 編集日時: 2022 年 1 月 17 日 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloud9SSMInstanceProfile

AWSCloud9SSMInstanceProfile は、InstanceProfile にロールをアタッチするために使用される AWS マネージドポリシーです。これにより、Cloud9 は、SSM Session Manager を使用してインスタンスに接続できるようになります。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloud9SSMInstanceProfile をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 5 月 14 日 11:40 UTC
- 編集日時: 2020 年 5 月 14 日 11:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloud9User

AWSCloud9User は、AWS Cloud9 開発環境の作成と、所有環境の管理許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloud9User をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 30 日 16:16 UTC
- 編集日時: 2023 年 10 月 11 日 13:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9User

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloudFormationFullAccess

`AWSCloudFormationFullAccess` は、AWS CloudFormation へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloudFormationFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 7 月 26 日 21:50 UTC
- 編集日時: 2019 年 7 月 26 日 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloudFormationReadOnlyAccess

`AWSCloudFormationReadOnlyAccess` は、AWS Management Console 経由で AWS CloudFormation へのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloudFormationReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2019 年 11 月 13 日 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloudFrontLogger

AWSCloudFrontLogger は、CloudFront Logger に CloudWatch Logs への書き込み権限を付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 6 月 12 日 20:15 UTC
- 編集日時: 2019 年 11 月 22 日 19:33 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloudHSMFullAccess

AWSCloudHSMFullAccess は、すべての CloudHSM リソースへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudHSMFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2015 年 2 月 6 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudHSMFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloudHSMReadOnlyAccess

`AWSCloudHSMReadOnlyAccess` は、すべての CloudHSM リソースへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloudHSMReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2015 年 2 月 6 日 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloudHSMRole

`AWSCloudHSMRole` は、AWS CloudHSM サービスロールのデフォルトポリシーとなる AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloudHSMRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloudMapDiscoverInstanceAccess

`AWSCloudMapDiscoverInstanceAccess` は、AWS クラウド Map discovery API へのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloudMapDiscoverInstanceAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 29 日 00:02 UTC
- 編集日時: 2023 年 9 月 20 日 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloudMapFullAccess

AWSCloudMapFullAccess は、すべての AWS クラウド マップアクションへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudMapFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 28 日 23:57 UTC
- 編集日時: 2020 年 7 月 29 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloudMapReadOnlyAccess

AWSCloudMapReadOnlyAccess は、すべての AWS クラウド マップアクションへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudMapReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 28 日 23:45 UTC
- 編集日時: 2023 年 9 月 20 日 21:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:Get*",
        "servicediscovery:List*",
```

```
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloudMapRegisterInstanceAccess

AWSCloudMapRegisterInstanceAccess は、登録者レベルのアクセス許可をすべての AWS クラウド マップアクションに提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudMapRegisterInstanceAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 29 日 00:04 UTC
- 編集日時: 2023 年 9 月 20 日 21:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloudShellFullAccess

AWSCloudShellFullAccess は、すべての機能を備えた AWS CloudShell の使用を許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudShellFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 15 日 18:07 UTC
- 編集日時: 2020 年 12 月 15 日 18:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudShellFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloudTrail_FullAccess

`AWSCloudTrail_FullAccess` は、AWS CloudTrail へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloudTrail_FullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 10 月 8 日 23:41 UTC
- 編集日時: 2021 年 2 月 22 日 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloudTrail_ReadOnlyAccess

`AWSCloudTrail_ReadOnlyAccess` は、AWS CloudTrail への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloudTrail_ReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 6 月 14 日 17:19 UTC
- 編集日時: 2022 年 6 月 14 日 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

`AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy` は、AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents というサービスリンクロールによって使用される AWS マネージドポリシーです。CloudWatch アラームが ALARM 状態になったときに AWS System Manager インシデントマネージャアクションを実行するために、このサービスリ

ンクロールを使用します。このポリシーは、ユーザーに代わってインシデントを開始するアクセス許可を付与します。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 4 月 27 日 13:30 UTC
- 編集日時: 2021 年 4 月 27 日 13:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeArtifactAdminAccess

`AWSCodeArtifactAdminAccess` は、AWS Management Console 経由で AWS CodeArtifact へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCodeArtifactAdminAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 6 月 16 日 23:53 UTC
- 編集日時: 2020 年 6 月 16 日 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeArtifactReadOnlyAccess

`AWSCodeArtifactReadOnlyAccess` は、AWS Management Console 経由で AWS CodeArtifact への読み取り専用アクセスを提供する AWS マネージドポリシー

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCodeArtifactReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 6 月 25 日 21:23 UTC
- 編集日時: 2020 年 6 月 25 日 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeBuildAdminAccess

AWSCodeBuildAdminAccess は、AWS Management Console 経由で AWS CodeBuild へのフルアクセスを提供する AWS マネージドポリシーです。また、AmazonS3ReadOnlyAccess をアタッチしてビルドアーティファクトをダウンロードできるようにしたり、IAMFullAccess をアタッチして CodeBuild のサービスロールを作成および管理したりすることもできます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeBuildAdminAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 12 月 1 日 19:04 UTC
- 編集日時: 2023 年 7 月 31 日 23:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess

ポリシーのバージョン

ポリシーのバージョン: v13 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeBuildDeveloperAccess

AWSCodeBuildDeveloperAccess は、AWS Management Console 経由で AWS CodeBuild へのアクセスを提供する AWS マネージドポリシーです。ただし、CodeBuild プロジェクト管理は許可しません。また、AmazonS3ReadOnlyAccess をアタッチして、ビルドアーティファクトをダウンロードできるようにします。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeBuildDeveloperAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 12 月 1 日 19:02 UTC
- 編集日時: 2023 年 7 月 31 日 23:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeBuildReadOnlyAccess

`AWSCodeBuildReadOnlyAccess` は、AWS Management Console 経由で AWS CodeBuild への読み取り専用アクセスを提供する AWS マネージドポリシーです。また、AmazonS3ReadOnlyAccess をアタッチして、ビルドアーティファクトをダウンロードできるようにします。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCodeBuildReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 12 月 1 日 19:03 UTC
- 編集日時: 2020 年 9 月 14 日 16:04 UTC

- ARN: arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeCommitFullAccess

`AWSCodeCommitFullAccess` は、AWS Management Console 経由で AWS CodeCommit へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeCommitFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 7 月 9 日 17:02 UTC
- 編集日時: 2023 年 7 月 17 日 21:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeCommitFullAccess

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeCommitPowerUser

AWSCodeCommitPowerUser は、AWS CodeCommit リポジトリへのフルアクセスを提供するAWS マネージドポリシーです。ただし、リポジトリの削除は許可しません。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeCommitPowerUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 7 月 9 日 17:06 UTC
- 編集日時: 2023 年 7 月 17 日 21:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeCommitPowerUser

ポリシーのバージョン

ポリシーのバージョン: v15 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeCommitReadOnly

`AWSCodeCommitReadOnly` は、AWS Management Console 経由で AWS CodeCommit への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeCommitReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 7 月 9 日 17:05 UTC
- 編集日時: 2021 年 8 月 18 日 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeCommitReadOnly

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeDeployDeployerAccess

AWSCodeDeployDeployerAccess は、リビジョンを登録してデプロイするためのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployDeployerAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 5 月 19 日 18:18 UTC
- 編集日時: 2020 年 4 月 2 日 16:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeDeployFullAccess

AWSCodeDeployFullAccess は、CodeDeploy リソースへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 5 月 19 日 18:13 UTC
- 編集日時: 2020 年 4 月 2 日 16:14 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeDeployReadOnlyAccess

AWSCodeDeployReadOnlyAccess は、CodeDeploy リソースへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 5 月 19 日 18:21 UTC
- 編集日時: 2020 年 4 月 2 日 16:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeDeployRole

AWSCodeDeployRole は、CodeDeploy サービスにアクセスしてタグを拡張し、ユーザーに代わって自動スケーリングを操作できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 5 月 4 日 18:05 UTC
- 編集日時: 2023 年 8 月 16 日 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole`

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeDeployRoleForCloudFormation

AWSCodeDeployRoleForCloudFormation は、ユーザーに代わって Lambda 関数を呼び出し、CloudFormation 経由でブルー/グリーンデプロイを実行するための CodeDeploy サービスアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployRoleForCloudFormation をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 5 月 19 日 17:12 UTC
- 編集日時: 2020 年 5 月 19 日 17:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
```

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeDeployRoleForECS

AWSCodeDeployRoleForECS は、ユーザーに代わって ECS ブルー/グリーンデプロイを実行するための CodeDeploy サービス全体へのアクセスを提供する AWS マネージドポリシーです。すべての S3 オブジェクトの読み取り、すべての Lambda 関数の呼び出し、アカウント内のすべての SNS トピックへの公開、すべての ECS サービスの更新など、サポートサービスへのフルアクセスを許可します。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployRoleForECS をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 27 日 20:40 UTC
- 編集日時: 2019 年 9 月 23 日 22:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeDeployRoleForECSLimited

AWSCodeDeployRoleForECSLimited は、ユーザーに代わって ECS ブルー/グリーンデプロイを実行するための限定アクセスを CodeDeploy サービスに提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployRoleForECSLimited をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 27 日 20:42 UTC
- 編集日時: 2019 年 9 月 23 日 22:10 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeDeployRoleForLambda

AWSCodeDeployRoleForLambda は、ユーザーに代わって Lambda デプロイを実行するための CodeDeploy サービスアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployRoleForLambda をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 11 月 28 日 14:05 UTC
- 編集日時: 2019 年 12 月 3 日 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeDeployRoleForLambdaLimited

AWSCodeDeployRoleForLambdaLimited は、ユーザーに代わって Lambda デプロイを実行するための制限のあるアクセス権を CodeDeploy サービスに提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployRoleForLambdaLimited をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 8 月 17 日 17:14 UTC
- 編集日時: 2020 年 8 月 17 日 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodePipeline_FullAccess

`AWSCodePipeline_FullAccess` は、経由で へのフルアクセスを提供する AWS マネージドポリシー AWS CodePipeline です AWS Management Console。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCodePipeline_FullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 8 月 3 日 22:38 UTC
- 編集日時： 2024 年 3 月 14 日 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSCodePipeline_ReadOnlyAccess

`AWSCodePipeline_ReadOnlyAccess` は、AWS Management Console 経由で AWS CodePipeline への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCodePipeline_ReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 8 月 3 日 22:25 UTC
- 編集日時: 2020 年 8 月 3 日 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodePipelineApproverAccess

AWSCodePipelineApproverAccess は、すべてのパイプラインの手動変更を表示および承認するためのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodePipelineApproverAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 7 月 28 日 18:59 UTC
- 編集日時: 2017 年 8 月 2 日 17:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodePipelineCustomActionAccess

AWSCodePipelineCustomActionAccess は、カスタムアクションがジョブ詳細をポーリング (一時的認証情報を含む) し、AWS CodePipeline へのステータス更新を報告するためのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodePipelineCustomActionAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 7 月 9 日 17:02 UTC
- 編集日時: 2015 年 7 月 9 日 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeStarFullAccess

AWSCodeStarFullAccess は、AWS Management Console 経由で AWS CodeStar へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeStarFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 4 月 19 日 16:23 UTC
- 編集日時: 2023 年 3 月 28 日 00:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeStarFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeStarNotificationsServiceRolePolicy

AWSCodeStarNotificationsServiceRolePolicy は、AWS CodeStar 通知がユーザーに代わって Amazon CloudWatch Events にアクセスすることを許可する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 5 日 16:10 UTC
- 編集日時: 2020 年 3 月 19 日 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCodeStarServiceRole

AWSCodeStarServiceRole という AWS マネージドポリシー は使用しないでください - AWS CodeStar サービスロールポリシーは、CodeStar がお客様に代わって IAM やその他のサービスリソースを管理するための管理者権限を付与するものです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeStarServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 4 月 19 日 15:20 UTC
- 編集日時: 2021 年 9 月 20 日 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole`

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCompromisedKeyQuarantine

AWSCompromisedKeyQuarantine は、IAM ユーザーの認証情報が漏えいしたり、公開されたりした場合に AWS チームによって適用される、特定のアクションへのアクセスを拒否するAWS マネージドポリシーです。このポリシーは削除しないでください。代わりに、このイベントに関して送信されたメールで指示されている手順に従ってください。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCompromisedKeyQuarantine をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 8 月 11 日 18:04 UTC
- 編集日時: 2020 年 8 月 11 日 18:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
```

```
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCompromisedKeyQuarantineV2

AWSCompromisedKeyQuarantineV2 は、IAM ユーザーの認証情報が漏えいしたり、公開されたりした場合に AWS チームによって適用される、特定のアクションへのアクセスを拒否するAWS マネージドポリシーです。このポリシーは削除しないでください。代わりに、このイベントに関して作成したサポートケースに明記されている指示に従ってください。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCompromisedKeyQuarantineV2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 4 月 21 日 22:30 UTC
- 編集日時: 2023 年 3 月 16 日 00:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSConfigMultiAccountSetupPolicy

AWSConfigMultiAccountSetupPolicy は、設定が AWS サービスを呼び出して組織全体で設定リソースを展開できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 17 日 18:03 UTC
- 編集日時: 2023 年 2 月 24 日 01:39 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSConfigRemediationServiceRolePolicy

AWSConfigRemediationServiceRolePolicy は、AWS 設定がユーザーに代わって準拠していないリソースを修正することを許可する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 18 日 21:21 UTC
- 編集日時: 2019 年 6 月 18 日 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
```

```
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSConfigRoleForOrganizations

AWSConfigRoleForOrganizations は、AWS 設定がが読み取り専用の AWS Organizations API を呼び出すことを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSConfigRoleForOrganizations をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 3 月 19 日 22:53 UTC
- 編集日時: 2020 年 11 月 24 日 20:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSConfigRulesExecutionRole

`AWSConfigRulesExecutionRole` は、AWS Lambda 関数が AWS Config API と、AWS Config が Amazon S3 に定期的に配信する設定スナップショットにアクセスできるようにする AWS マネージドポリシーです。このアクセスは、カスタム Config ルールの設定変更を評価する関数に必要です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSConfigRulesExecutionRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 3 月 25 日 17:59 UTC
- 編集日時: 2019 年 5 月 13 日 21:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSConfigServiceRolePolicy

AWSConfigServiceRolePolicy は、Config がユーザーに代わって AWS サービスを呼び出し、リソース設定を収集できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 5 月 30 日 23:31 UTC
- 編集日時： 2024 年 2 月 22 日 17:20 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v50 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
```

```
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSConfigUserAccess

AWSConfigUserAccess は、AWS 設定を使用するためのアクセス権 (例: タグによるリソース検索、すべてのタグの読み取り) をユーザーに付与する AWS マネージドポリシーです。このポリシーでは、AWS Config を設定するアクセス許可は付与されません。このアクセス許可には管理者権限が必要です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSConfigUserAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 18 日 19:38 UTC
- 編集日時: 2019 年 3 月 18 日 20:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSConfigUserAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSConnector

`AWSConnector` は、 AWS コネクタがユーザーに代わって VMs をインポートするために、すべての EC2 オブジェクトへの広範な読み取り/書き込みアクセス、import-to-ec「2-」で始まる S3 バケットへの読み取り/書き込みアクセス、およびすべての S3 バケットを一覧表示する機能を有効にする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSConnector` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 11 日 17:14 UTC
- 編集日時: 2015 年 9 月 28 日 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConnector`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSControlTowerAccountServiceRolePolicy

AWSControlTowerAccountServiceRolePolicy は、AWS Control Tower が、ユーザーに代わって自動アカウント設定と一元管理を行う AWS サービスを呼び出すことができるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 6 月 5 日 22:04 UTC
- 編集日時: 2023 年 6 月 5 日 22:04 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSControlTowerServiceRolePolicy

AWSControlTowerServiceRolePolicy は、AWS Control Tower が管理または使用する AWS リソースへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSControlTowerServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 5 月 3 日 18:19 UTC
- 編集日時: 2023 年 4 月 12 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSCostAndUsageReportAutomationPolicy

AWSCostAndUsageReportAutomationPolicy は、アカウントの組織を記述する権限、MAP プログラム用の S3 バケットの作成とタグの適用、コストと使用状況レポートの作成、コストと使用状況レポートの定義の説明を行う権限を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCostAndUsageReportAutomationPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 1 日 21:27 UTC
- 編集日時: 2021 年 11 月 1 日 21:27 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDataExchangeFullAccess

AWSDataExchangeFullAccess は、AWS Management Console および SDK を使用した AWS Data Exchange および AWS Marketplace アクションへのフルアクセスを許可する AWS マネージドポリシーです。また、AWS Data Exchange を最大限に活用するために必要な関連サービスへの選択したアクセスも提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDataExchangeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 11 月 13 日 19:27 UTC
- 編集日時: 2021 年 12 月 2 日 16:14 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDataExchangeProviderFullAccess

`AWSDataExchangeProviderFullAccess` は、AWS Management Console および SDK を使用する AWS Data Exchange と AWS Marketplace アクションへのアクセス権をデータプロバイダーに付与する AWS マネージドポリシーです。また、AWS Data Exchange を最大限に活用するために必要な関連サービスへの選択したアクセスも提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDataExchangeProviderFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 11 月 13 日 19:27 UTC
- 編集日時: 2022 年 3 月 15 日 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDataExchangeReadOnly

`AWSDataExchangeReadOnly` は、AWS Management Console および SDK を使用する AWS Data Exchange と AWS Marketplace アクションへの読み取り専用アクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDataExchangeReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 11 月 13 日 19:27 UTC
- 編集日時: 2021 年 5 月 10 日 21:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeReadOnly

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDataExchangeSubscriberFullAccess

`AWSDataExchangeSubscriberFullAccess` は、AWS Management Console および SDK を使用した AWS Data Exchange と AWS Marketplace アクションへのデータサブスクライバーアクセスを許可する AWS マネージドポリシーです。また、AWS Data Exchange を最大限に活用するために必要な関連サービスへの選択したアクセスも提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDataExchangeSubscriberFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 11 月 13 日 19:27 UTC
- 編集日時: 2021 年 11 月 29 日 23:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDataLifecycleManagerServiceRole

AWSDataLifecycleManagerServiceRole は、AWS リソースに対してアクションを実行するための適切なアクセス許可を AWS Data Lifecycle Manager に付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDataLifecycleManagerServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 7 月 6 日 19:34 UTC
- 編集日時: 2022 年 9 月 19 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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.*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDataLifecycleManagerServiceRoleForAMIManagement

`AWSDataLifecycleManagerServiceRoleForAMIManagement` は、AMI 管理用の AWS リソースに対してアクションを実行するための適切な権限を AWS Data Lifecycle Manager に提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDataLifecycleManagerServiceRoleForAMIManagement` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 10 月 21 日 19:39 UTC
- 編集日時: 2021 年 8 月 19 日 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDataLifecycleManagerSSMFullAccess

`AWSDataLifecycleManagerSSMFullAccess` は、すべての Amazon EC2 インスタンスでプリスクリプトとポストスクリプトを実行するために必要な Systems Manager アクションを実行するための Amazon Data Lifecycle Manager のアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDataLifecycleManagerSSMFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 10 月 31 日 20:29 UTC
- 編集時間:2023 年 11 月 16 日 22:31 UTC

- ARN: arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDataPipeline_FullAccess

`AWSDataPipeline_FullAccess` は、Data Pipeline へのフルアクセス、S3、DynamoDB、Redshift、RDS、SNS、IAM ロールへのリストアクセス、デフォルトロールの passRole アクセスを提供する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDataPipeline_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 1 月 19 日 23:14 UTC
- 編集日時: 2017 年 8 月 17 日 18:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDataPipeline_PowerUser

`AWSDataPipeline_PowerUser` は、Data Pipeline へのフルアクセス、S3、DynamoDB、Redshift、RDS、SNS、IAM ロールへのリストアクセス、デフォルトロールの passRole アクセスを提供する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDataPipeline_PowerUser` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 1 月 19 日 23:16 UTC

- 編集日時: 2017 年 8 月 17 日 18:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDataSyncDiscoveryServiceRolePolicy

AWSDataSyncDiscoveryServiceRolePolicy は、ユーザーに代わって DataSync Discovery を他の AWS サービスと統合できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 3 月 20 日 22:19 UTC
- 編集日時: 2023 年 3 月 20 日 22:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
      ]
    }
```

```
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDataSyncFullAccess

AWSDataSyncFullAccess は、 へのフルアクセス AWS DataSync と依存関係への最小限のアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDataSyncFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 1 月 18 日 19:40 UTC
- 編集日時： 2024 年 2 月 16 日 17:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataSyncFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
          ]
```

```
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSDataSyncReadOnlyAccess

`AWSDataSyncReadOnlyAccess` は、AWS DataSync への読み取り専用アクセスを提供するAWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDataSyncReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 1 月 18 日 19:18 UTC
- 編集日時: 2020 年 6 月 30 日 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDeepLensLambdaFunctionAccessPolicy

`AWSDeepLensLambdaFunctionAccessPolicy` は、DeepLens デバイス上で実行される DeepLens 管理用 Lambda 関数に必要なアクセス許可を指定する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepLensLambdaFunctionAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 29 日 15:47 UTC
- 編集日時: 2019 年 6 月 11 日 23:11 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDeepLensServiceRolePolicy

AWSDeepLensServiceRolePolicy は、AWS DeepLens とその依存関係に必要な AWS のサービス、リソースとロール (IoT、S3 、GreenGrass、AWS Lambda など) へのアクセスを許可する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepLensServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 11 月 29 日 15:46 UTC
- 編集日時: 2019 年 9 月 25 日 19:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDeepRacerAccountAdminAccess

AWSDeepRacerAccountAdminAccess は、マルチユーザーモードとシングルユーザーモードの切り替えを含むすべてのアクションへの DeepRacer 管理者アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepRacerAccountAdminAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 10 月 28 日 01:27 UTC
- 編集日時: 2021 年 10 月 28 日 01:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDeepRacerCloudFormationAccessPolicy

AWSDeepRacerCloudFormationAccessPolicy は、CloudFormation がユーザーに代わって AWS スタックとリソースを作成および管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepRacerCloudFormationAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 2 月 28 日 21:59 UTC
- 編集日時: 2019 年 6 月 14 日 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDeepRacerDefaultMultiUserAccess

AWSDeepRacerDefaultMultiUserAccess は、DeepRacer MultiUser マルチユーザーマルチユーザーモードで Deepracer を使用するためのデフォルトのユーザーのアクセス権である AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepRacerDefaultMultiUserAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 10 月 28 日 01:27 UTC
- 編集日時: 2021 年 10 月 28 日 01:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDeepRacerFullAccess

`AWSDeepRacerFullAccess` は、AWS DeepRacer へのフルアクセスを提供する AWS マネージドポリシーです。また、関連サービス (S3 など) への限定アクセスも提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDeepRacerFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 10 月 5 日 22:03 UTC
- 編集日時: 2020 年 10 月 5 日 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*/*"
```

```
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDeepRacerRoboMakerAccessPolicy

AWSDeepRacerRoboMakerAccessPolicy は、RoboMaker がお客様に代わって必要なリソースを作成して AWS サービスを呼び出すことを許可する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepRacerRoboMakerAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 2 月 28 日 21:59 UTC
- 編集日時: 2019 年 2 月 28 日 21:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDeepRacerServiceRolePolicy

AWSDeepRacerServiceRolePolicy は、お客様に代わって DeepRacer 必要なリソースを作成して AWS サービスを呼び出すことを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepRacerServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 2 月 28 日 21:58 UTC
- 編集日時: 2019 年 6 月 12 日 20:55 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDenyAll

AWSDenyAll は、すべてのアクセスを拒否する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDenyAll をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 5 月 1 日 22:36 UTC
- 編集時間:2023 年 12 月 18 日 16:42 UTC
- ARN: arn:aws:iam::aws:policy/AWSDenyAll

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDeviceFarmFullAccess

AWSDeviceFarmFullAccess は、AWS Device Farm のすべての操作へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeviceFarmFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 7 月 13 日 16:37 UTC
- 編集日時: 2015 年 7 月 13 日 16:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDeviceFarmServiceRolePolicy

AWSDeviceFarmServiceRolePolicy は、ユーザーに代わって EC2 ネットワーク API を呼び出すアクセス許可を AWS Device Farm に付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 9 月 20 日 21:02 UTC
- 編集日時: 2022 年 9 月 20 日 21:02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDeviceFarmTestGridServiceRolePolicy

AWSDeviceFarmTestGridServiceRolePolicy は、ユーザーに代わって EC2 API を呼び出すアクセス許可を AWS Device Farm に付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 5 月 26 日 22:01 UTC
- 編集日時: 2021 年 5 月 26 日 22:01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDirectConnectFullAccess

`AWSDirectConnectFullAccess` は、AWS Management Console 経由で AWS Direct Connect へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDirectConnectFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2019 年 4 月 30 日 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDirectConnectReadOnlyAccess

`AWSDirectConnectReadOnlyAccess` は、AWS Management Console 経由で AWS Direct Connect への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDirectConnectReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2020 年 5 月 18 日 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDirectConnectServiceRolePolicy

AWSDirectConnectServiceRolePolicy は、ユーザーに代わって AWS リソースを作成および管理するための AWS Direct Connect のアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 1 月 14 日 18:35 UTC
- 編集日時: 2021 年 1 月 14 日 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
```

```
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDirectoryServiceFullAccess

AWSDirectoryServiceFullAccess は、AWS Directory Service へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDirectoryServiceFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2020 年 11 月 24 日 23:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDirectoryServiceReadOnlyAccess

`AWSDirectoryServiceReadOnlyAccess` は、AWS Directory Service への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDirectoryServiceReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2018 年 9 月 25 日 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
```

```
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDiscoveryContinuousExportFirehosePolicy

AWSDiscoveryContinuousExportFirehosePolicy は、AWS Discovery の継続的エクスポートに必要な AWS リソースへの書き込みアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDiscoveryContinuousExportFirehosePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 8 月 9 日 18:29 UTC
- 編集日時: 2021 年 6 月 8 日 17:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDMSFleetAdvisorServiceRolePolicy

AWSDMSFleetAdvisorServiceRolePolicy は、DMS フリートアドバイザーがユーザーに代わって CloudWatch メトリクスを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 3 月 6 日 09:10 UTC
- 編集日時: 2023 年 3 月 6 日 09:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/DMS/FleetAdvisor"
      }
    }
  }
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSDMSServerlessServiceRolePolicy

AWSDMSServerlessServiceRolePolicy は、ユーザーに代わってアカウント内の AWS DMS リソースを作成および管理する権限を DMS サーバーレスに付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 5 月 18 日 20:28 UTC
- 編集日時: 2023 年 5 月 18 日 20:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSEC2CapacityReservationFleetRolePolicy

AWSEC2CapacityReservationFleetRolePolicy は、EC2 CapacityReservation Fleet サービスにキャパシティ予約の管理を許可する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 9 月 29 日 14:43 UTC
- 編集日時: 2021 年 9 月 29 日 14:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSEC2FleetServiceRolePolicy

AWSEC2FleetServiceRolePolicy は、EC2 フリートにインスタンスの起動と管理を許可する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 3 月 21 日 00:08 UTC
- 編集日時: 2020 年 5 月 4 日 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSEC2SpotFleetServiceRolePolicy

AWSEC2SpotFleetServiceRolePolicy は、EC2 スポットフリートにスポットフリートインスタンスの起動と管理を許可する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 23 日 19:13 UTC
- 編集日時: 2020 年 3 月 16 日 19:16 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*:*:*/*"
```

```
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSEC2SpotServiceRolePolicy

AWSEC2SpotServiceRolePolicy は、EC2 スポットがスポットインスタンスを起動して管理することを許可する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 18 日 18:51 UTC
- 編集日時: 2018 年 12 月 12 日 00:13 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSECRPullThroughCache_ServiceRolePolicy

AWSECRPullThroughCache_ServiceRolePolicy は、AWS ECR プルスルーキャッシュが使用または管理するサービスと AWS リソースへのアクセスを可能にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2021 年 11 月 26 日 21:51 UTC
- 編集日時: 2023 年 11 月 13 日 15:23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
```

```
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticBeanstalkCustomPlatformforEC2Role

AWSElasticBeanstalkCustomPlatformforEC2Role は、EC2 インスタンスの起動、EBS スナップショットと AMI の作成、Amazon CloudWatch Logs へのログのストリーミング、Amazon S3 へのアーティファクトの保存を行うためのアクセス許可をカスタムプラットフォームビルダー環境のインスタンスに提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkCustomPlatformforEC2Role をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 2 月 21 日 22:50 UTC
- 編集日時: 2017 年 2 月 21 日 22:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticBeanstalkEnhancedHealth

`AWSElasticBeanstalkEnhancedHealth` は、ヘルスモニタリングシステム向けの AWS Elastic Beanstalk サービスポリシーである AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkEnhancedHealth をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 2 月 8 日 23:17 UTC
- 編集日時: 2018 年 4 月 9 日 22:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticBeanstalkMaintenance

`AWSElasticBeanstalkMaintenance` は、ユーザーに代わってメンテナンスの目的でリソースを更新する限定的なアクセス権限を付与する AWS Elastic Beanstalk サービスである AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 1 月 11 日 23:22 UTC
- 編集日時: 2019 年 6 月 4 日 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy は、AWS Elastic Beanstalk 環境のマネージドアップデートを実行するために使用される Elastic Beanstalk サービスロール用 AWS マネージドポリシーです。このポリシーは他のユーザーやロールには適用しないでください。このポリシーは、AutoScaling、EC2、ECS、Elastic Load Balancing、CloudFormation など、さまざまな AWS サービスにわたってリソースを作成および管理するための幅広いアクセス許可を付与します。このポリシーでは、それらのサービスで使用可能なすべての IAM ロールを渡すことも許可されます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 3 月 3 日 22:18 UTC
- 編集日時: 2023 年 3 月 23 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy は、制限付きのアクセス権限を付与する AWS Elastic Beanstalk サービスロールポリシーである AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 21 日 22:35 UTC
- 編集日時: 2023 年 3 月 24 日 00:18 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticBeanstalkMulticontainerDocker

AWSElasticBeanstalkMulticontainerDocker は、マルチコンテナの Docker 環境のインスタンスに Amazon EC2 Container Service を使用してコンテナデプロイタスクを管理するためのアクセス権を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkMulticontainerDocker をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 2 月 8 日 23:15 UTC
- 編集日時: 2023 年 3 月 23 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticBeanstalkReadOnly

AWSElasticBeanstalkReadOnly は、読み取り専用権限を付与する AWS マネージドポリシーです。オペレーターが直接アクセスして AWS Elastic Beanstalk アプリケーションに関連するリソースに関する情報を取得することを明示的に許可します。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 1 月 22 日 19:02 UTC
- 編集日時: 2021 年 1 月 22 日 19:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticBeanstalkRoleCore

AWSElasticBeanstalkRoleCore は、AWSElasticBeanstalkRoleCore (Elastic Beanstalk オペレーションロール) であり、ウェブサービス環境のコアオペレーションを許可する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkRoleCore をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 5 日 21:48 UTC
- 編集日時: 2020 年 9 月 9 日 20:31 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticBeanstalkRoleCWL

AWSElasticBeanstalkRoleCWL は、Elastic Beanstalk オペレーションロールであり、環境が Amazon CloudWatch Logs ロググループを管理することを許可する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkRoleCWL をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 5 日 21:49 UTC
- 編集日時: 2020 年 6 月 5 日 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticBeanstalkRoleECS

AWSElasticBeanstalkRoleECS は、Elastic Beanstalk オペレーションロールであり、複数コンテナの Docker 環境で Amazon ECS クラスターを管理できるようにする AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkRoleECS をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 5 日 21:47 UTC
- 編集日時: 2023 年 3 月 23 日 22:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticBeanstalkRoleRDS

AWSElasticBeanstalkRoleRDS は、Elastic Beanstalk オペレーションロールであり、環境が Amazon RDS インスタンスを統合することを許可する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkRoleRDS をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 5 日 21:46 UTC
- 編集日時: 2020 年 6 月 5 日 21:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticBeanstalkRoleSNS

AWSElasticBeanstalkRoleSNS は、Elastic Beanstalk オペレーションロールであり、環境が Amazon SNS トピック統合を有効にすることを許可する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkRoleSNS をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 5 日 21:46 UTC
- 編集日時: 2020 年 6 月 5 日 21:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticBeanstalkRoleWorkerTier

`AWSElasticBeanstalkRoleWorkerTier` は、Elastic Beanstalk オペレーションロールであり、ワーカー環境階層が Amazon DynamoDB テーブルと Amazon SQS キューを作成することを許可する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkRoleWorkerTier をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 5 日 21:43 UTC
- 編集日時: 2020 年 6 月 5 日 21:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticBeanstalkService

AWSElasticBeanstalkService は、廃止予定の AWS マネージドポリシーです。ガイダンスについては、「https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html」にあるドキュメントを参照してください。 AWSユーザーに代わってリソース (AutoScaling、EC2、S3、CloudFormation、ELB など) を作成および管理するためのアクセス許可を付与する Elastic Beanstalk サービスロールポリシー。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkService をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 4 月 11 日 20:27 UTC
- 編集日時: 2023 年 5 月 10 日 19:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService

ポリシーのバージョン

ポリシーのバージョン: v17 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticBeanstalkServiceRolePolicy

`AWSElasticBeanstalkServiceRolePolicy` は、ユーザーに代わってリソース (AutoScaling、EC2、S3、CloudFormation、ELB など) を作成および管理する権限を付与する AWS Elastic Beanstalk サービスリンクロールポリシーである AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 13 日 23:46 UTC
- 編集日時: 2019 年 6 月 6 日 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticBeanstalkWebTier

AWSElasticBeanstalkWebTier は、ウェブサーバー環境のインスタンスに Amazon S3 にログファイルをアップロードするためのアクセス権を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkWebTier をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 2 月 8 日 23:08 UTC
- 編集日時: 2020 年 9 月 9 日 19:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticBeanstalkWorkerTier

AWSElasticBeanstalkWorkerTier は、ワーカー環境のインスタンスに Amazon S3 へのログファイルのアップロード、Amazon SQS によるアプリケーションのジョブキューのモニタリング、Amazon DynamoDB によるリーダー選定の実行、Amazon CloudWatch へのヘルスモニタリングのためのメトリクス公開を行うためのアクセスを付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkWorkerTier をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 2 月 8 日 23:12 UTC
- 編集日時: 2020 年 9 月 9 日 19:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticDisasterRecoveryAgentInstallationPolicy

`AWSElasticDisasterRecoveryAgentInstallationPolicy` は、外部サーバーを AWS へリカバリするために AWS Elastic Disaster Recovery (DRS) と併用される AWS レプリケーションエージェントをインストールできるようにする AWS マネージドポリシーです。このポリシーは、AWS レプリケーションエージェントのインストール手順で認証情報を入力した IAM ユーザーまたはロールにアタッチしてください。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticDisasterRecoveryAgentInstallationPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 17 日 10:37 UTC
- 編集時間:2023 年 11 月 27 日 12:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticDisasterRecoveryAgentPolicy

AWSElasticDisasterRecoveryAgentPolicy は、AWS Elastic Disaster Recovery (DRS) と併用される AWS レプリケーションエージェントを使用してソースサーバーを AWS へ復旧できるようにする AWS マネージドポリシーです。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryAgentPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 17 日 10:32 UTC
- 編集時間:2023 年 11 月 27 日 13:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticDisasterRecoveryConsoleFullAccess

`AWSElasticDisasterRecoveryConsoleFullAccess` は、AWS Elastic Disaster Recovery (DRS) のすべてのパブリック API へのフルアクセス権のほか、KMS キー、License Manager、Resource Groups、Elastic Load Balancing、IAM、EC2 情報を読み取るアクセス許可を付与する AWS マネージドポリシーです。このポリシーを IAM ユーザーまたはロールにアタッチします。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticDisasterRecoveryConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 17 日 10:46 UTC
- 編集日時: 2023 年 10 月 16 日 12:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticDisasterRecoveryConsoleFullAccess_v2

AWSElasticDisasterRecoveryConsoleFullAccess_v2AWSは次のような管理ポリシーです。このポリシーは、AWS Elastic Disaster Recovery（AWSDRS）のすべてのパブリックAPIと、AWS AWS DRSコンソールが使用する他のサービスのすべてのパブリックAPIへのフルアクセスを提供します。このポリシーをユーザーまたはロールに添付してください。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryConsoleFullAccess_v2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時間:2023 年 11 月 27 日 13:35 UTC
- 編集時間:2023 年 11 月 27 日 13:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticDisasterRecoveryConversionServerPolicy

`AWSElasticDisasterRecoveryConversionServerPolicy` は、AWS Elastic Disaster Recovery Conversion サーバーのインスタンスロールにアタッチされる AWS マネージドポリシーです。このポリシーにより、Elastic Disaster Recovery (DRS) コンバージョンサーバー (Elastic Disaster Recovery によって起動される EC2 インスタンス) が DRS サービスと通信できるようになります。このポリシーが適用された IAM ロールは DRS によって DRS 変換サーバーに (EC2 インスタンスプロファイルとして) アタッチされます。DRS 変換サーバーは、必要に応じて DRS によって自動的に起動および終了されます。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。DRS 変換サーバーは、ユーザーが DRS コンソール、CLI、または API を使用してソースサーバーを復元することを選択したときに、Elastic Disaster Recovery によって使用されます。

このポリシーを使用すると

ユーザー、グループおよびロールに
AWSElasticDisasterRecoveryConversionServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 17 日 13:42 UTC
- 編集時間:2023 年 11 月 27 日 13:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/
  AWSElasticDisasterRecoveryConversionServerPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy は、AWS Elastic Disaster Recovery (DRS) が、クロスアカウントレプリケーションとクロスアカウントフェールバックをサポートできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryCrossAccountReplicationPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 5 月 14 日 07:16 UTC
- 編集日時： 2024 年 1 月 17 日 13:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticDisasterRecoveryEc2InstancePolicy

AWSElasticDisasterRecoveryEc2InstancePolicy は、AWS Elastic Disaster Recovery (DRS) が EC2 (クロスリージョンまたは Cross-AZ) AWS 上で稼働するソースサーバーを復旧するために使用するレプリケーションエージェントのインストールと使用を許可する AWS マネージドポリシーです。このポリシーを含む IAM ロールは、EC2 インスタンスに (EC2 インスタンスプロファイルとして) アタッチする必要があります。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryEc2InstancePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 5 月 26 日 12:30 UTC
- 編集時間:2023 年 11 月 27 日 13:39 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticDisasterRecoveryFailbackInstallationPolicy

AWSElasticDisasterRecoveryFailbackInstallationPolicyは、AWS次のような管理ポリシーです。 AWSElasticDisasterRecoveryFailbackInstallationPolicy ポリシーを IAM ID にアタッチできます。このポリシーにより、リカバリーインスタンスを元のソースインフラストラクチャにフェールバックするために使用される Elastic Disaster Recovery Failback Client のインストールが可能になります。このポリシーを、Elastic Disaster Recovery Failback Client の実行時に提供した認証情報を持つ IAM ユーザーまたはロールにアタッチしてください。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryFailbackInstallationPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 17 日 11:02 UTC
- 編集時間:2023 年 11 月 27 日 13:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticDisasterRecoveryFailbackPolicy

`AWSElasticDisasterRecoveryFailbackPolicy` は、リカバリーインスタンスを元のソースインフラストラクチャにフェールバックするために使用される Elastic Disaster Recovery フェイルバッククライアントの使用を許可する AWS マネージドポリシーです。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryFailbackPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 17 日 10:41 UTC
- 編集時間:2023 年 11 月 27 日 12:56 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticDisasterRecoveryLaunchActionsPolicy

AWSElasticDisasterRecoveryLaunchActionsPolicy は、Amazon SSM やその他のサービスに必要なアクセス権限を使用して、AWS Elastic Disaster Recovery (AWSDRS) で起動後のアクションを実行できるようにする AWS マネージドポリシーです。このポリシーを IAM ロールまたはユーザーにアタッチします。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryLaunchActionsPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 9 月 13 日 07:38 UTC
- 編集日時: 2023 年 10 月 16 日 12:28 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticDisasterRecoveryNetworkReplicationPolicy

`AWSElasticDisasterRecoveryNetworkReplicationPolicy` は、AWS Elastic Disaster Recovery (DRS) がネットワークレプリケーションをサポートできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに
AWSElasticDisasterRecoveryNetworkReplicationPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 6 月 11 日 12:36 UTC
- 編集日時： 2024 年 1 月 2 日 13:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/
  AWSElasticDisasterRecoveryNetworkReplicationPolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticDisasterRecoveryReadOnlyAccess

AWSElasticDisasterRecoveryReadOnlyAccessは、AWS次のような管理ポリシーです。AWSElasticDisasterRecoveryReadOnlyAccess ポリシーを IAM ID にアタッチできます。このポリシーは、Elastic Disaster Recovery (DRS) の全ての読み取り専用パブリック API へのアクセス許可および、DRS コンソールの完全な読み取り専用使用のために必要な他の AWS の一部の読み取り専用 API へのアクセス許可を付与します。このポリシーを IAM ユーザーまたはロールにアタッチします。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 17 日 10:50 UTC
- 編集時間:2023 年 11 月 27 日 13:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticDisasterRecoveryRecoveryInstancePolicy

`AWSElasticDisasterRecoveryRecoveryInstancePolicy` は、Elastic Disaster Recovery の Recovery インスタンスのインスタンスロールにアタッチされる AWS マネージドポリシーです。このポリシーにより、Elastic Disaster Recovery によって起動された EC2 インスタンスである Elastic Disaster Recovery (DRS) Recovery インスタンスが DRS サービスと通信し、元のソースインフラストラクチャにフェイルバックできるようになります。このポリシーが適用された IAM ロールは、Elastic Disaster Recovery によって DRS Recovery インスタンスに (EC2 インスタンスプロファイルとして) アタッチされます。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticDisasterRecoveryRecoveryInstancePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 17 日 10:20 UTC

- 編集時間:2023 年 11 月 27 日 13:11 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticDisasterRecoveryReplicationServerPolicy

AWSElasticDisasterRecoveryReplicationServerPolicy は、Elastic Disaster Recovery Replication サーバーのインスタンスロールにアタッチされる AWS マネージドポリシーです。このポリシーは、Elastic Disaster Recovery によって起動された EC2 インスタンスである Elastic Disaster Recovery (DRS) レプリケーションサーバーが DRS サービスと通信し、AWS アカウントに EBS スナップショットを作成することを許可します。このポリシーが適用された IAM ロールは Elastic Disaster Recovery によって DRS レプリケーションサーバーに (EC2 インスタンスプロファイルとして) アタッチされます。必要に応じて DRS によって自動的に起動および終了されます。DRS レプリケーションサーバーは、DRS が管理する復旧プロセスの一環として、外部サーバーから AWS へのデータ複製を容易にするために使用されます。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryReplicationServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 17 日 13:34 UTC
- 編集時間:2023 年 11 月 27 日 13:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticDisasterRecoveryServiceRolePolicy

AWSElasticDisasterRecoveryServiceRolePolicy は、Elastic Disaster AWS Recovery がユーザーに代わってリソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 17 日 10:56 UTC
- 編集日時： 2024 年 1 月 17 日 13:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticDisasterRecoveryStagingAccountPolicy

AWSElasticDisasterRecoveryStagingAccountPolicy は、ソースサーバーやジョブなどの AWS Elastic Disaster Recovery (DRS) リソースへの読み取り専用アクセスを許可する AWS マネージドポリシーです。また、変換されたスナップショットを作成し、その EBS スナップショットを特定のアカウントと共有することもできます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryStagingAccountPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2022 年 5 月 26 日 09:49 UTC
- 編集時間:2023 年 11 月 27 日 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

AWSElasticDisasterRecoveryStagingAccountPolicy_v2 は、AWS Elastic Disaster Recovery (DRS) がソースサーバーを別のターゲットアカウントに復元し、フェールバックを可能にするために使用される AWS マネージドポリシーです。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryStagingAccountPolicy_v2 をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 1 月 5 日 12:11 UTC
- 編集時間:2023 年 11 月 27 日 13:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント


```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticLoadBalancingClassicServiceRolePolicy

`AWSElasticLoadBalancingClassicServiceRolePolicy` は、AWS Elastic Load Balancing コントロールプレーン (Classic) のサービスリンクロールポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 19 日 22:36 UTC
- 編集日時: 2019 年 10 月 7 日 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElasticLoadBalancingServiceRolePolicy

AWSElasticLoadBalancingServiceRolePolicy は、AWS Elastic Load Balancing コントロールプレーンのサービスリンクロールポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 19 日 22:19 UTC
- 編集日時: 2021 年 8 月 26 日 19:01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElementalMediaConvertFullAccess

AWSElementalMediaConvertFullAccess は、AWS Management Console および SDK 経由で AWS Elemental MediaConvert へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaConvertFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 6 月 25 日 19:25 UTC
- 編集日時: 2019 年 6 月 10 日 22:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElementalMediaConvertReadOnly

`AWSElementalMediaConvertReadOnly` は、AWS Management Console および SDK 経由で AWS Elemental MediaConvert への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElementalMediaConvertReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 6 月 25 日 19:25 UTC
- 編集日時: 2019 年 6 月 10 日 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:DescribeEndpoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElementalMediaLiveFullAccess

AWSElementalMediaLiveFullAccess は、AWS Elemental MediaLive リソースへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaLiveFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 7 月 8 日 17:07 UTC
- 編集日時: 2020 年 7 月 8 日 17:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElementalMediaLiveReadOnly

`AWSElementalMediaLiveReadOnly` は、AWS Elemental MediaLive リソースへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElementalMediaLiveReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 7 月 8 日 16:38 UTC
- 編集日時: 2020 年 7 月 8 日 16:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "medialive:List*",
      "medialive:Describe*"
    ],
    "Resource" : "*"
  }
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElementalMediaPackageFullAccess

`AWSElementalMediaPackageFullAccess` は、AWS Elemental MediaPackage リソースへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElementalMediaPackageFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 12 月 29 日 23:39 UTC
- 編集日時: 2017 年 12 月 29 日 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElementalMediaPackageReadOnly

`AWSElementalMediaPackageReadOnly` は、AWS Elemental MediaPackage リソースへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElementalMediaPackageReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 12 月 30 日 00:04 UTC
- 編集日時: 2017 年 12 月 30 日 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElementalMediaPackageV2FullAccess

`AWSElementalMediaPackageV2FullAccess` は、AWS Elemental MediaPackageV2 リソースへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElementalMediaPackageV2FullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 7 月 25 日 20:29 UTC
- 編集日時: 2023 年 7 月 25 日 20:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElementalMediaPackageV2ReadOnly

`AWSElementalMediaPackageV2ReadOnly` は、AWS Elemental MediaPackageV2 リソースへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaPackageV2ReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 7 月 25 日 20:31 UTC
- 編集日時: 2023 年 7 月 25 日 20:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElementalMediaStoreFullAccess

AWSElementalMediaStoreFullAccess は、すべての MediaStore API への完全な読み取りおよび書き込みアクセスを提供する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaStoreFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 3 月 5 日 23:15 UTC
- 編集日時: 2018 年 3 月 5 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:*"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElementalMediaStoreReadOnly

`AWSElementalMediaStoreReadOnly` は、MediaStore API に読み取り専用のアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElementalMediaStoreReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 3 月 8 日 19:48 UTC
- 編集日時: 2018 年 3 月 8 日 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElementalMediaTailorFullAccess

`AWSElementalMediaTailorFullAccess` は、AWS Elemental MediaTailor リソースへのフルアクセスを提供する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaTailorFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 23 日 00:04 UTC
- 編集日時: 2021 年 11 月 23 日 00:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSElementalMediaTailorReadOnly

AWSElementalMediaTailorReadOnly は、AWS Elemental MediaTailor リソースへの読み取り専用アクセスを提供する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaTailorReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 23 日 00:05 UTC
- 編集日時: 2021 年 11 月 23 日 00:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSEnhancedClassicNetworkingMangementPolicy

AWSEnhancedClassicNetworkingMangementPolicy は、拡張クラシックネットワーク管理機能を有効にするポリシーです。 AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 20 日 17:29 UTC
- 編集日時: 2017 年 9 月 20 日 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSEntityResolutionConsoleFullAccess

AWSEntityResolutionConsoleFullAccess は、AWS Entity Resolution および関連サービスへのフルアクセスをコンソールに提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSEntityResolutionConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 8 月 17 日 17:54 UTC
- 編集日時: 2023 年 10 月 16 日 18:46 UTC
- ARN: arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSEntityResolutionConsoleReadOnlyAccess

AWSEntityResolutionConsoleReadOnlyAccess は、AWS Management Console 経由で AWS エンティティ解決への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSEntityResolutionConsoleReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 8 月 17 日 18:18 UTC
- 編集日時: 2023 年 8 月 17 日 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSFaultInjectionSimulatorEC2Access

`AWSFaultInjectionSimulatorEC2Access` は、EC2 およびその他の必要なサービスで FIS アクションを実行するためのアクセス許可を Fault Injection Simulator サービスに付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSFaultInjectionSimulatorEC2Access` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 26 日 20:39 UTC
- 編集時間:2023 年 11 月 27 日 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSFaultInjectionSimulatorECSAccess

AWSFaultInjectionSimulatorECSAccess は、Fault Injection Simulator サービスに、FIS アクションを実行するための ECS およびその他の必要なサービスのアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSFaultInjectionSimulatorECSAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 26 日 20:37 UTC
- 編集日時： 2024 年 1 月 25 日 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSFaultInjectionSimulatorEKSAccess

`AWSFaultInjectionSimulatorEKSAccess` は、EKS およびその他の必要なサービスの Fault Injection Simulator サービスに FIS アクションを実行するためのアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSFaultInjectionSimulatorEKSAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 26 日 20:34 UTC
- 編集日時: 2023 年 11 月 13 日 16:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSFaultInjectionSimulatorNetworkAccess

`AWSFaultInjectionSimulatorNetworkAccess` は、EC2 ネットワーキングおよびその他の必要なサービスで FIS アクションを実行するためのアクセス許可を Fault Injection Simulator サービスに付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSFaultInjectionSimulatorNetworkAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 26 日 20:32 UTC
- 編集日時： 2024 年 1 月 25 日 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSFaultInjectionSimulatorRDSAccess

AWSFaultInjectionSimulatorRDSAccess は、RDS の Fault Injection Simulator サービスに、FIS アクションを実行するためのその他の必要なサービスのアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSFaultInjectionSimulatorRDSAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 26 日 20:30 UTC
- 編集日時: 2023 年 11 月 13 日 16:23 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
```

```
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSFaultInjectionSimulatorSSMAccess

AWSFaultInjectionSimulatorSSMAccess は、SSM の Fault Injection Simulator サービスに FIS アクションを実行するためのアクセス許可およびその他の必要なサービスを付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSFaultInjectionSimulatorSSMAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 26 日 15:33 UTC
- 編集日時: 2023 年 6 月 2 日 22:55 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSFinSpaceServiceRolePolicy

AWSFinSpaceServiceRolePolicyは、Amazon AWSAWS のサービスが使用または管理するリソースへのアクセスを有効にするポリシーです。 FinSpace

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 5 月 12 日 16:42 UTC
- 編集時間:2023 年 12 月 1 日 21:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSFMAdminFullAccess

AWSFMAdminFullAccess は、AWS FM 管理者向けのフルアクセス権である AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSFMAdminFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 5 月 9 日 18:06 UTC
- 編集日時: 2022 年 10 月 20 日 23:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSFMAdminFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSFMAdminReadOnlyAccess

AWSFMAdminReadOnlyAccess は、AWS FM 管理者の読み取り専用アクセス権で、AWS FM 操作の監視を許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSFMAdminReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 5 月 9 日 20:07 UTC
- 編集日時: 2022 年 10 月 31 日 22:42 UTC
- ARN: arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント


```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSFMMemberReadOnlyAccess

`AWSFMMemberReadOnlyAccess` は、AWS Firewall Manager メンバーアカウントに AWS WAF アクションへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSFMMemberReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 5 月 9 日 21:05 UTC
- 編集日時: 2018 年 5 月 9 日 21:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSForWordPressPluginPolicy

AWSForWordPressPluginPolicy は、Wordpress プラグイン用 AWS のマネージドポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSForWordPressPluginPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 10 月 30 日 00:27 UTC
- 編集日時: 2020 年 1 月 20 日 23:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSGitSyncServiceRolePolicy

`AWSGitSyncServiceRolePolicy` は、AWS Code Connections が Git リポジトリのコンテンツを同期することを許可する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 16 日 17:05 UTC
- 編集日時: 2023 年 11 月 16 日 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
```

```
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSGlobalAcceleratorSLRPolicy

AWSGlobalAcceleratorSLRPolicy は、EC2 Elastic Network インターフェイスとセキュリティグループを管理する権限を AWS Global Accelerator に付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 4 月 5 日 19:39 UTC
- 編集日時: 2023 年 9 月 12 日 16:45 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSGlueConsoleFullAccess

`AWSGlueConsoleFullAccess` は、AWS Management Console 経由で AWS Glue へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSGlueConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 8 月 14 日 13:37 UTC
- 編集日時: 2023 年 7 月 14 日 14:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSGlueConsoleSageMakerNotebookFullAccess

AWSGlueConsoleSageMakerNotebookFullAccess は、AWS Management Console 経由で AWS Glue へのフルアクセスと Sagemaker ノートブックインスタンスへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGlueConsoleSageMakerNotebookFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 10 月 5 日 17:52 UTC
- 編集日時: 2021 年 7 月 15 日 15:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント


```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AwsGlueDataBrewFullAccessPolicy

`AwsGlueDataBrewFullAccessPolicy` は、AWS Management Console 経由で AWS Glue DataBrew へのフルアクセスを提供する AWS マネージドポリシーです。また、関連サービス (S3、KMS、Glue など) への特定のアクセスも提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AwsGlueDataBrewFullAccessPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 11 月 11 日 16:51 UTC
- 編集日時: 2022 年 2 月 4 日 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSGlueDataBrewServiceRole

AWSGlueDataBrewServiceRole は、ユーザーのグルーデータカタログでアクションを実行するアクセス許可をグルーに付与する AWS マネージドポリシー です。また、このポリシーは、グルーが VPC 内のリソースに接続するための ENI を作成できるようにする権限を ec2 アクションに付与し、グルーが lakeformation の登録データにアクセスできるようにし、ユーザーの cloudwatch へのアクセス許可も付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGlueDataBrewServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 4 日 21:26 UTC
- 編集日時： 2024 年 3 月 20 日 23:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSGlueSchemaRegistryFullAccess

AWSGlueSchemaRegistryFullAccess は、AWS Glue Schema レジストリサービスへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGlueSchemaRegistryFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 11 月 20 日 00:19 UTC
- 編集日時: 2020 年 11 月 20 日 00:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSGlueSchemaRegistryReadonlyAccess

AWSGlueSchemaRegistryReadonlyAccess は、AWS Glue Schema レジストリサービスへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGlueSchemaRegistryReadonlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 11 月 20 日 00:20 UTC
- 編集日時: 2020 年 11 月 20 日 00:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadonlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSGlueServiceNotebookRole

AWSGlueServiceNotebookRole は、お客様がノートブックサーバーを管理できるようにする AWS Glue サービスロールである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGlueServiceNotebookRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 8 月 14 日 13:37 UTC
- 編集日時: 2023 年 10 月 9 日 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSGlueServiceRole

AWSGlueServiceRole は、EC2、S3、Cloudwatch Logs などの関連サービスへのアクセスを許可する AWS Glue サービスロールの AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGlueServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 8 月 14 日 13:37 UTC
- 編集日時: 2023 年 9 月 11 日 16:39 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AwsGlueSessionUserRestrictedNotebookPolicy

AwsGlueSessionUserRestrictedNotebookPolicy は、ユーザー自身に関連付けられているノートブックセッションのみを作成および使用できるようにするアクセス許可を提供する AWS マネージドポリシーです。このポリシーには、ユーザーが制限付き Glue セッションロールを渡すことを明示的に許可するアクセス許可も含まれます。

このポリシーを使用すると

ユーザー、グループおよびロールに AwsGlueSessionUserRestrictedNotebookPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 4 月 18 日 15:24 UTC
- 編集時間:2023 年 11 月 22 日 01:32 UTC
- ARN: arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AwsGlueSessionUserRestrictedNotebookServiceRole

AwsGlueSessionUserRestrictedNotebookServiceRole は、セッションを除くすべての AWS Glue リソースへのフルアクセスを許可するAWS マネージドポリシーです。ユーザーが、ユーザーに関連付けられているノートブックセッションのみを作成して使用できるようにします。このポリシーには、他の AWS サービスで Glue リソースを管理するために、AWS Glue が必要とするその他のアクセス許可も含まれています。

このポリシーを使用すると

ユーザー、グループおよびロールに AwsGlueSessionUserRestrictedNotebookServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 4 月 18 日 15:27 UTC
- 編集日時: 2022 年 4 月 18 日 15:27 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AwsGlueSessionUserRestrictedPolicy

AwsGlueSessionUserRestrictedPolicy は、ユーザーに関連付けられたインタラクティブセッションのみ、作成と使用を許可するアクセス許可を提供する AWS マネージドポリシーです。このポリシーには、ユーザーが制限付き Glue セッションロールを渡すことを明示的に許可するアクセス許可も含まれます。

このポリシーを使用すると

ユーザー、グループおよびロールに AwsGlueSessionUserRestrictedPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 4 月 14 日 21:31 UTC
- 編集日時: 2022 年 4 月 14 日 21:31 UTC
- ARN: arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AwsGlueSessionUserRestrictedServiceRole

AwsGlueSessionUserRestrictedServiceRole は、セッションを除くすべての AWS Glue リソースへのフルアクセスを許可するAWS マネージドポリシーです。ユーザーは、そのユーザーに関連付けられている対話型セッションのみを作成して使用できるようにします。このポリシーには、他の AWS サービスで Glue リソースを管理するために、AWS Glue が必要とするその他のアクセス許可も含まれています。

このポリシーを使用すると

ユーザー、グループおよびロールに AwsGlueSessionUserRestrictedServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 4 月 14 日 21:30 UTC
- 編集日時: 2022 年 4 月 14 日 21:30 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSGrafanaAccountAdministrator

`AWSGrafanaAccountAdministrator` は、組織全体のワークスペースを作成および管理するための Amazon Grafana 内のアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSGrafanaAccountAdministrator` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 2 月 23 日 00:20 UTC
- 編集日時: 2022 年 2 月 15 日 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSGrafanaConsoleReadOnlyAccess

`AWSGrafanaConsoleReadOnlyAccess` は、Amazon Grafana の読み取り専用オペレーションへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSGrafanaConsoleReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 2 月 23 日 00:10 UTC
- 編集日時: 2022 年 2 月 15 日 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSGrafanaWorkspacePermissionManagement

`AWSGrafanaWorkspacePermissionManagement` は、AWS Grafana ワークスペースのユーザーのアクセス許可とグループのアクセス許可を更新する機能のみを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSGrafanaWorkspacePermissionManagement` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2021 年 2 月 23 日 00:15 UTC
- 編集日時: 2023 年 3 月 15 日 22:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSGrafanaWorkspacePermissionManagementV2

AWSGrafanaWorkspacePermissionManagementV2 は、Amazon Managed Grafana ワークスペースの IAM Identity Center (IdC) ユーザーおよびグループのアクセス許可を更新する機能を提供する マネージドAWSポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGrafanaWorkspacePermissionManagementV2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時刻: 2024 年 1 月 5 日 18:39 UTC
- 編集日時： 2024 年 1 月 5 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSGreengrassFullAccess

`AWSGreengrassFullAccess` は、AWS Greengrass の設定、管理、および導入アクションへのフルアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSGreengrassFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 5 月 3 日 00:47 UTC
- 編集日時: 2017 年 5 月 3 日 00:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "greengrass:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSGreengrassReadOnlyAccess

AWSGreengrassReadOnlyAccess は、AWS Greengrass の設定、管理、およびデプロイアクションへの読み取り専用アクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGreengrassReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 10 月 30 日 16:01 UTC
- 編集日時: 2018 年 10 月 30 日 16:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSGreengrassResourceAccessRolePolicy

`AWSGreengrassResourceAccessRolePolicy` は、AWS Lambda や AWS IoT Thing Shadow などの関連サービスへのアクセスを許可する AWS Greengrass サービスロールの AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSGreengrassResourceAccessRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 2 月 14 日 21:17 UTC
- 編集日時: 2018 年 11 月 14 日 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSGroundStationAgentInstancePolicy

`AWSGroundStationAgentInstancePolicy` は、データフローエンドポイントインスタンスに AWS Ground Station Agent を使用する権限を提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGroundStationAgentInstancePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 3 月 29 日 15:23 UTC
- 編集日時: 2023 年 3 月 29 日 15:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSHealth_EventProcessorServiceRolePolicy

AWSHealth_EventProcessorServiceRolePolicy は、AWS Health がヘルスイベントプロセッサ機能を有効にできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 1 月 13 日 19:24 UTC
- 編集日時: 2023 年 1 月 13 日 19:24 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSHealthFullAccess

AWSHealthFullAccess は、AWS Health API および通知と、Personal Health Dashboard へのフルアクセスを付与する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSHealthFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 12 月 6 日 12:30 UTC
- 編集日時: 2020 年 11 月 16 日 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSHealthImagingFullAccess

`AWSHealthImagingFullAccess` は、AWS Health イメージングサービスへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSHealthImagingFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 7 月 25 日 23:39 UTC
- 編集日時: 2023 年 7 月 25 日 23:39 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSHealthImagingReadOnlyAccess

AWSHealthImagingReadOnlyAccess は、AWS Health イメージングサービスへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSHealthImagingReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 7 月 25 日 23:40 UTC
- 編集日時: 2023 年 8 月 1 日 15:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIAMIdentityCenterAllowListForIdentityContext

`AWSIAMIdentityCenterAllowListForIdentityContext` は、IAM アイデンティティセンター ID コンテキストので引き受けられるロールに許可されるアクションのリストを提供するAWS マネージドポリシーです。AWSセキュリティトークンサービス (AWS STS) は、このポリシーを引き受けたロールに自動的にアタッチします。ID コンテキストはとして渡されます ProvidedContext。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIAMIdentityCenterAllowListForIdentityContext` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 11 月 8 日 15:21 UTC
- 編集時間:2023 年 11 月 25 日 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント


```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIdentitySyncFullAccess

`AWSIdentitySyncFullAccess` は、Identity Sync サービスへのフルアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIdentitySyncFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 3 月 23 日 23:29 UTC
- 編集日時: 2022 年 3 月 23 日 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*:*:*/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIdentitySyncReadOnlyAccess

`AWSIdentitySyncReadOnlyAccess` は、Identity Sync サービスへの読み取り専用アクセス権を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIdentitySyncReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 3 月 23 日 23:29 UTC
- 編集日時: 2022 年 3 月 23 日 23:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSImageBuilderFullAccess

AWSImageBuilderFullAccess は、AWS Image Builder のすべてのアクションへのフルアクセスと、関連 AWS サービスへのリソーススコープのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSImageBuilderFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 20 日 18:25 UTC
- 編集日時: 2021 年 4 月 13 日 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSImageBuilderFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSImageBuilderReadOnlyAccess

`AWSImageBuilderReadOnlyAccess` は、AWS Image Builder のすべてのアクションへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSImageBuilderReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 19 日 22:29 UTC
- 編集日時: 2019 年 12 月 19 日 22:29 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSImportExportFullAccess

AWSImportExportFullAccess は、AWS アカウント で作成されたジョブへの読み取りおよび書き込みアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSImportExportFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSImportExportFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSImportExportReadOnlyAccess

AWSImportExportReadOnlyAccess は、AWS アカウント で作成されたジョブには読み取り専用アクセス権を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSImportExportReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "importexport:ListJobs",
        "importexport:GetStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIncidentManagerIncidentAccessServiceRolePolicy

`AWSIncidentManagerIncidentAccessServiceRolePolicy` は、インシデントの管理の一環として他の AWS のサービスを呼び出すアクセス許可を Incident Manager に付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIncidentManagerIncidentAccessServiceRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 11 月 13 日 00:01 UTC
- 編集日時： 2024 年 2 月 20 日 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSIncidentManagerResolverAccess

AWSIncidentManagerResolverAccess は、インシデントを開始、表示、更新するアクセス許可と、カスタムタイムラインイベントおよび関連項目へのフルアクセス権を付与する AWS マネージドポリシーです。インシデントを作成および解決するユーザーにこのポリシー割り当ててください。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIncidentManagerResolverAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 5 月 10 日 06:12 UTC
- 編集日時: 2021 年 5 月 10 日 06:12 UTC
- ARN: arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIncidentManagerServiceRolePolicy

`AWSIncidentManagerServiceRolePolicy` は、ユーザーに代わって Indent Manager に Incident レコードと関連リソースを管理するアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 5 月 10 日 03:34 UTC
- 編集日時: 2022 年 12 月 5 日 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoT1ClickFullAccess

AWSIoT1ClickFullAccess は、AWS IoT 1-Click へのフルアクセスを提供する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoT1ClickFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 5 月 11 日 22:10 UTC
- 編集日時: 2018 年 5 月 11 日 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoT1ClickReadOnlyAccess

AWSIoT1ClickReadOnlyAccess は、AWS IoT 1-Click への読み取り専用アクセスを提供する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoT1ClickReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 5 月 11 日 21:49 UTC
- 編集日時: 2018 年 5 月 11 日 21:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTAnalyticsFullAccess

`AWSIoTAnalyticsFullAccess` は、IoT Analytics へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTAnalyticsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 6 月 18 日 23:02 UTC
- 編集日時: 2018 年 6 月 18 日 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotanalytics:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTAnalyticsReadOnlyAccess

AWSIoTAnalyticsReadOnlyAccess は、IoT Analytics への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTAnalyticsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 6 月 18 日 21:37 UTC
- 編集日時: 2018 年 6 月 18 日 21:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTConfigAccess

`AWSIoTConfigAccess` は、AWS IoT 設定アクションへのフルアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTConfigAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 10 月 27 日 21:52 UTC
- 編集日時: 2019 年 9 月 27 日 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigAccess`

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTConfigReadOnlyAccess

`AWSIoTConfigReadOnlyAccess` は、AWS IoT 設定アクションへの読み取り専用アクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTConfigReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 10 月 27 日 21:52 UTC
- 編集日時: 2019 年 9 月 27 日 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTDataAccess

`AWSIoTDataAccess` は、AWS IoT メッセージングアクションへのフルアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTDataAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 10 月 27 日 21:51 UTC
- 編集日時: 2021 年 6 月 23 日 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDataAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

`AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` は、ADD_THINGS_TO_THING_GROUP 緩和アクションを実行するための IoT Thing グループへの書き込みアクセスと IoT 証明書への読み取りアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2019 年 8 月 7 日 17:55 UTC
- 編集日時: 2019 年 8 月 7 日 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTDeviceDefenderAudit

AWSIoTDeviceDefenderAudit は、IoT および関連リソースへの読み取りアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTDeviceDefenderAudit をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 7 月 18 日 21:17 UTC
- 編集日時: 2019 年 11 月 25 日 23:52 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

`AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction` は、ENABLE_IOT_LOGGING 緩和アクションを実行するための IoT ロギングを有効にするためのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 8 月 7 日 17:04 UTC
- 編集日時: 2019 年 8 月 7 日 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : [
            "iot.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction は、PUBLISH_FINDING_TO_SNS 緩和アクションを実行するための SNS トピックへのメッセージ公開アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 8 月 7 日 17:04 UTC
- 編集日時: 2019 年 8 月 7 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

`AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction` は、REPLACE_DEFAULT_POLICY_VERSION 緩和アクションを実行するための IoT ポリシーへの書き込みアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 8 月 7 日 17:04 UTC
- 編集日時: 2019 年 8 月 7 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTDeviceDefenderUpdateCACertMitigationAction

AWSIoTDeviceDefenderUpdateCACertMitigationAction は、UPDATE_CA_CERTIFICATE 緩和アクションを実行するための IoT CA 証明書への書き込みアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTDeviceDefenderUpdateCACertMitigationAction をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 8 月 7 日 17:05 UTC
- 編集日時: 2019 年 8 月 7 日 17:05 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

`AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction` は、UPDATE_DEVICE_CERTIFICATE 緩和アクションを実行するための IoT 証明書への書き込みアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 8 月 7 日 17:06 UTC
- 編集日時: 2019 年 8 月 7 日 17:06 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTDeviceTesterForFreeRTOSFullAccess

AWSIoTDeviceTesterForFreeRTOSFullAccess は、IoT、S3、IAM などのサービスへのアクセスを許可することで、AWS IoT デバイステスターが FreeRTOS 認定スイートを実行できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTDeviceTesterForFreeRTOSFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 2 月 12 日 20:33 UTC
- 編集日時: 2023 年 8 月 10 日 20:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTDeviceTesterForGreengrassFullAccess

AWSIoTDeviceTesterForGreengrassFullAccess は、Lambda、IoT、API Gateway、IAM などの関連サービスへのアクセスを許可することで、AWS IoT Device Tester が AWS Greengrass 認定スイートを実行できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTDeviceTesterForGreengrassFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 2 月 20 日 21:21 UTC
- 編集日時: 2020 年 6 月 25 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTEventsFullAccess

`AWSIoTEventsFullAccess` は、IoT Events へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTEventsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 1 月 10 日 22:51 UTC
- 編集日時: 2019 年 1 月 10 日 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTEventsReadOnlyAccess

AWSIoTEventsReadOnlyAccess は、IoT イベントへの読み取り専用アクセスを提供する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTEventsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 1 月 10 日 22:50 UTC
- 編集日時: 2019 年 9 月 23 日 17:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTFleetHubFederationAccess

`AWSIoTFleetHubFederationAccess` は、IoT Fleet Hub アプリケーションのフェデレーションアクセスとなる AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTFleetHubFederationAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 15 日 08:08 UTC
- 編集日時: 2022 年 4 月 4 日 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTFleetHubFederationAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTFleetwiseServiceRolePolicy

AWSIoTFleetwiseServiceRolePolicy は、AWSIotFleetWise が使用または管理する AWS リソースとメタデータへのアクセス許可を補助機能として付与する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 9 月 21 日 23:27 UTC
- 編集日時: 2022 年 9 月 21 日 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTFleetwiseServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTFullAccess

`AWSIoTFullAccess` は、AWS IoT 設定とメッセージングアクションへのフルアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 10 月 8 日 15:19 UTC
- 編集日時: 2022 年 5 月 19 日 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:*",
        "iotjobsdata:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTLogging

AWSIoTLogging は、Amazon CloudWatch Log グループを作成し、そのグループにログをストリーミングすることを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTLogging をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 10 月 8 日 15:17 UTC
- 編集日時: 2015 年 10 月 8 日 15:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTLogging

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTOTAUpdate

`AWSIoTOTAUpdate` は、AWS IoT ジョブを作成し、AWS コード署名ジョブを記述するためのアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTOTAUpdate をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 12 月 20 日 20:36 UTC
- 編集日時: 2017 年 12 月 20 日 20:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIotRoboRunnerFullAccess

AWSIotRoboRunnerFullAccess は、AWS IoT RoboRunner への完全なアクセスを可能にするアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIotRoboRunnerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 29 日 03:54 UTC
- 編集日時: 2023 年 2 月 23 日 18:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSIotRoboRunnerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIotRoboRunnerReadOnly

AWSIotRoboRunnerReadOnly は、AWS IoT RoboRunner への読み取り専用アクセスを可能にするアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIotRoboRunnerReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 29 日 03:43 UTC
- 編集日時: 2022 年 11 月 16 日 20:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSIotRoboRunnerReadOnly

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIotRoboRunnerServiceRolePolicy

`AWSIotRoboRunnerServiceRolePolicy` は、AWS IoT RoboRunner が顧客に代わって関連 AWS リソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 2 月 21 日 16:56 UTC
- 編集日時: 2023 年 2 月 21 日 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIotRoboRunnerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  }
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTRuleActions

AWSIoTRuleActions は、AWS IoT Rule Actions でサポートされるすべての AWS サービスへのアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTRuleActions をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 10 月 8 日 15:14 UTC
- 編集日時: 2018 年 1 月 16 日 19:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
  }
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTSiteWiseConsoleFullAccess

`AWSIoTSiteWiseConsoleFullAccess` は、AWS Management Console を使用して AWS IoT SiteWise を管理するためのフルアクセスを提供する AWS マネージドポリシーです。このポリシーでは、AWS IoT SiteWise (AWS IoT Analytics など) で使用されるデータストアの作成と一覧表示、AWS IoT Greengrass リソースの一覧表示と表示、AWS Secrets Manager シークレットの一覧表示と変更、AWS IoT Thing シャドウの取得、特定のタグが付いたリソースの一覧表示、AWS IoT SiteWise のサービスリンクロールの作成と使用に関するアクセス許可も付与されることに注意してください。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTSiteWiseConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 5 月 31 日 21:37 UTC
- 編集日時: 2019 年 5 月 31 日 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTSiteWiseFullAccess

`AWSIoTSiteWiseFullAccess` は、IoT SiteWise へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTSiteWiseFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 12 月 4 日 20:53 UTC

- 編集日時: 2018 年 12 月 4 日 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTSiteWiseMonitorPortalAccess

`AWSIoTSiteWiseMonitorPortalAccess` は、AWS IoT SiteWise のアセットとアセットデータへのアクセス、AWS IoT SiteWise Monitor リソースの作成、AWS SSO ユーザーの一覧表示を行うアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTSiteWiseMonitorPortalAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 5 月 19 日 20:01 UTC
- 編集日時: 2020 年 5 月 19 日 20:01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTSiteWiseMonitorServiceRolePolicy

`AWSIoTSiteWiseMonitorServiceRolePolicy` は、AWS IoT SiteWise のアセットとアセットプロパティにアクセスし、AWS IoT SiteWise ポータル経由で AWS IoT Sitewise プロジェクト、ダッシュボード、アクセスポリシーを作成するための権限を AWS IoT SiteWise モニターに付与するロールである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 14 日 00:59 UTC
- 編集日時: 2019 年 12 月 13 日 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTSiteWiseReadOnlyAccess

`AWSIoTSiteWiseReadOnlyAccess` は、IoT SiteWise への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTSiteWiseReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 12 月 4 日 20:55 UTC

- 編集日時: 2022 年 9 月 16 日 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTThingsRegistration

AWSIoTThingsRegistration は、ユーザーが AWS IoT StartThingRegistrationTask API を使用してモノを一括登録できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTThingsRegistration をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 12 月 1 日 20:21 UTC
- 編集日時: 2020 年 10 月 5 日 19:20 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTTwinMakerServiceRolePolicy

AWSIoTTwinMakerServiceRolePolicyは、AWS IoT TwinMaker AWS がユーザーに代わって他のサービスを呼び出したり、AWSそれらのリソースを同期したりできるようにする管理ポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 13 日 18:59 UTC
- 編集日時: 2023 年 11 月 13 日 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTTwinMakerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTWirelessDataAccess

AWSIoTWirelessDataAccess は、関連する ID データに AWS IoT Wireless デバイスへのアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTWirelessDataAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 15 日 15:31 UTC
- 編集日時: 2020 年 12 月 15 日 15:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTWirelessFullAccess

AWSIoTWirelessFullAccess は、関連付けられた ID にすべての AWS IoT Wireless 操作へのフルアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTWirelessFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 15 日 15:27 UTC
- 編集日時: 2020 年 12 月 15 日 15:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTWirelessFullPublishAccess

`AWSIoTWirelessFullPublishAccess` は、ユーザーに代わって IoT Rules Engine にパブリッシュするためのフルアクセス権を IoT Wireless に付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTWirelessFullPublishAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 15 日 15:29 UTC
- 編集日時: 2020 年 12 月 15 日 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTWirelessGatewayCertManager

AWSIoTWirelessGatewayCertManager は、関連付けられた ID アクセスに、IoT 証明書を作成、一覧表示、および記述することを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTWirelessGatewayCertManager をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 15 日 15:30 UTC
- 編集日時: 2020 年 12 月 15 日 15:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTWirelessLogging

AWSIoTWirelessLogging は、関連付けられた ID に Amazon CloudWatch Logs グループと、グループへのストリーミングログの作成を許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTWirelessLogging をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 15 日 15:32 UTC
- 編集日時: 2020 年 12 月 15 日 15:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessLogging

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIoTWirelessReadOnlyAccess

`AWSIoTWirelessReadOnlyAccess` は、AWS IoT ワイヤレスへの読み取り専用アクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTWirelessReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 15 日 15:28 UTC

- 編集日時: 2020 年 12 月 15 日 15:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIPAMServiceRolePolicy

`AWSIPAMServiceRolePolicy` は、VPC IP アドレスマネージャーがユーザーに代わって VPC リソースにアクセスし、AWS Organizations と統合できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 30 日 19:08 UTC
- 編集日時: 2023 年 11 月 8 日 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIQContractServiceRolePolicy

AWSIQContractServiceRolePolicy は、AWS IQ が顧客に代わって支払いリクエストを実行するために使用する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 8 月 22 日 19:28 UTC
- 編集日時: 2019 年 8 月 22 日 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIQFullAccess

AWSIQFullAccess は、AWS IQ へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIQFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 4 月 4 日 23:13 UTC
- 編集日時: 2019 年 9 月 25 日 20:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSIQFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSIQPermissionServiceRolePolicy

AWSIQPermissionServiceRolePolicy は、AWS IQ の専門家が担う役割を AWS IQ が管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2019 年 8 月 22 日 19:36 UTC
- 編集日時: 2019 年 8 月 22 日 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy は、AWS KMS カスタムキーストアに必要な AWS サービスとリソースへのアクセスを可能にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 14 日 20:10 UTC
- 編集日時: 2023 年 11 月 10 日 19:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

`AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy` は、AWS KMS がマルチリージョンキーの共有プロパティを同期できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 6 月 16 日 15:37 UTC
- 編集日時: 2021 年 6 月 16 日 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSKeyManagementServicePowerUser

AWSKeyManagementServicePowerUser は、AWS キー管理サービス (KMS) へのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSKeyManagementServicePowerUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2017 年 3 月 7 日 00:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLakeFormationCrossAccountManager

`AWSLakeFormationCrossAccountManager` は、Lake Formation 経由で Glue リソースへのクロスアカウントアクセスを提供する AWS マネージドポリシーです。組織やリソースアクセスマネージャーなど、他の必要なサービスへの読み取りアクセスも付与します

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSLakeFormationCrossAccountManager` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2020 年 8 月 4 日 20:59 UTC
- 編集日時: 2023 年 11 月 1 日 00:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
```

```
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLakeFormationDataAdmin

AWSLakeFormationDataAdmin は、データレイクを管理するための、AWS Lake Formation および関連サービス（AWS Glue など）への管理アクセスを付与する AWS マネージドポリシーです

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLakeFormationDataAdmin をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 8 月 8 日 17:33 UTC
- 編集日時: 2019 年 12 月 16 日 22:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLambda_FullAccess

AWSLambda_FullAccess は、AWS Lambda サービス、AWS Lambda コンソール機能、その他の関連 AWS サービスへのフルアクセスを付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambda_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 11 月 17 日 21:14 UTC
- 編集日時: 2020 年 11 月 17 日 21:14 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambda_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLambda_ReadOnlyAccess

AWSLambda_ReadOnlyAccess は、AWS Lambda サービス、AWS Lambda コンソール機能、その他関連 AWS サービスへの読み取り専用のアクセスを付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambda_ReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 11 月 17 日 21:10 UTC
- 編集日時: 2023 年 7 月 27 日 17:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLambdaBasicExecutionRole

`AWSLambdaBasicExecutionRole` は、CloudWatch ログへの書き込み許可を提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSLambdaBasicExecutionRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 4 月 9 日 15:03 UTC
- 編集日時: 2015 年 4 月 9 日 15:03 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLambdaDynamoDBExecutionRole

`AWSLambdaDynamoDBExecutionRole` は、DynamoDB ストリームへのリストと読み取りアクセスを提供し、CloudWatch ログへの書き込み許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaDynamoDBExecutionRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 4 月 9 日 15:09 UTC
- 編集日時: 2015 年 4 月 9 日 15:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLambdaENIManagementAccess

AWSLambdaENIManagementAccess は、VPC 対応の Lambda 関数が使用する ENI (作成、記述、削除) を管理するための、最低限の許可を Lambda 関数に提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaENIManagementAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 12 月 6 日 00:37 UTC
- 編集日時: 2020 年 10 月 1 日 20:07 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLambdaExecute

`AWSLambdaExecute` は、プット、S3 へのアクセス取得、CloudWatch ログへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSLambdaExecute` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaExecute`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLambdaFullAccess

AWSLambdaFullAccess は、廃止予定の AWS マネージドポリシーです。ガイダンスについては、「https://docs.aws.amazon.com/lambda/latest/dg/access-control-identity-based.html」のドキュメントを参照してください。Lambda、S3、DynamoDB、CloudWatch メトリクス、ログへのフルアクセスを提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2017 年 11 月 27 日 23:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaFullAccess

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLambdaInvocation-DynamoDB

AWSLambdaInvocation-DynamoDB は、DynamoDB Streams への読み取りアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaInvocation-DynamoDB をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLambdaKinesisExecutionRole

AWSLambdaKinesisExecutionRole は、Kinesis ストリームへのリストおよび読み取りアクセスを提供し、CloudWatch ログへの書き込み許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaKinesisExecutionRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 4 月 9 日 15:14 UTC
- 編集日時: 2018 年 11 月 19 日 20:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLambdaMSKExecutionRole

AWSLambdaMSKExecutionRole は VPC 内の MSK クラスターへのアクセス、VPC 内の ENI 管理 (作成、記述、削除)、CloudWatch ログへの書き込みに必要なアクセス権限を提供する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaMSKExecutionRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 8 月 11 日 17:35 UTC
- 編集日時: 2022 年 8 月 2 日 20:08 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLambdaReplicator

AWSLambdaReplicator は、Lambda Replicator がリージョン間で関数をレプリケートするために必要な許可を付与する AWS マネージドポリシーです

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 5 月 23 日 17:53 UTC
- 編集日時: 2017 年 12 月 8 日 00:17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLambdaRole

AWSLambdaRole は、AWS Lambda サービスロールのデフォルトポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLambdaSQSQueueExecutionRole

AWSLambdaSQSQueueExecutionRole は。SQS キューへのメッセージ受信、メッセージ削除、属性の読み取りアクセス、および CloudWatch ログへの書き込み許可を提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaSQSQueueExecutionRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 6 月 14 日 21:50 UTC
- 編集日時: 2018 年 6 月 14 日 21:50 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLambdaVPCAccessExecutionRole

AWSLambdaVPCAccessExecutionRole は、VPC 内のリソースにアクセスする際に Lambda 関数が実行する最小限のアクセス許可を提供する AWSマネージドポリシーです。ネットワークインターフェイスの作成、記述、削除、および CloudWatch Logs への書き込みのアクセス許可です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaVPCAccessExecutionRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 2 月 11 日 23:15 UTC
- 編集日時： 2024 年 1 月 5 日 22:38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLicenseManagerConsumptionPolicy

AWSLicenseManagerConsumptionPolicy は、ユーザーが資格を持つライセンスで使用するために必要な AWS License Manager API アクションへのアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLicenseManagerConsumptionPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 8 月 11 日 23:18 UTC
- 編集日時: 2021 年 8 月 11 日 23:18 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

`AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy` は、AWS License Manager Linux サブスクリプションサービスがユーザーに代わってリソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 12 月 20 日 18:54 UTC
- 編集日時: 2022 年 12 月 20 日 18:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLicenseManagerMasterAccountRolePolicy

AWSLicenseManagerMasterAccountRolePolicy は、AWS License Manager サービスマスターのアカウントロールポリシーである AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 26 日 19:03 UTC
- 編集日時: 2022 年 5 月 31 日 20:50 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLicenseManagerMemberAccountRolePolicy

`AWSLicenseManagerMemberAccountRolePolicy` は、AWS License Manager サービスメンバーのアカウントロールである AWS マネージドポリシーです

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 26 日 19:04 UTC
- 編集日時: 2019 年 11 月 15 日 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLicenseManagerServiceRolePolicy

AWSLicenseManagerServiceRolePolicy は、AWS License Manager サービスのデフォルトロールである AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 26 日 19:02 UTC
- 編集日時: 2021 年 7 月 30 日 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

AWSLicenseManagerUserSubscriptionsServiceRolePolicy は、AWS License Manager User Subscriptions サービスがユーザーに代わってリソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 7 月 30 日 01:17 UTC
- 編集日時: 2022 年 11 月 21 日 19:51 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSM2ServicePolicy

AWSM2ServicePolicy は、AWS M2 がユーザーに代わって AWS リソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 6 月 7 日 20:26 UTC
- 編集日時: 2022 年 6 月 7 日 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSManagedServices_ContactsServiceRolePolicy

AWSManagedServices_ContactsServiceRolePolicy は、AWS Managed Services が AWS リソース上のタグの値を読み取りできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 3 月 23 日 17:07 UTC
- 編集日時: 2023 年 3 月 23 日 17:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy は、AWS マネージドサービスが発見的制御インフラストラクチャを管理することに関する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2022 年 12 月 19 日 23:11 UTC
- 編集日時: 2022 年 12 月 19 日 23:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSManagedServices_EventsServiceRolePolicy

AWSManagedServices_EventsServiceRolePolicy は、AMS イベントプロセッサ機能を有効にする AWS マネージドサービスの AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 2 月 7 日 18:41 UTC
- 編集日時: 2023 年 2 月 7 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSManagedServicesDeploymentToolkitPolicy

`AWSManagedServicesDeploymentToolkitPolicy` は、AWS Managed Services がユーザーに代わってデプロイツールキットを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 6 月 9 日 18:33 UTC
- 編集日時: 2023 年 5 月 10 日 17:48 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMarketplaceAmiIngestion

AWSMarketplaceAmiIngestion は、AWS Marketplace に出品するために AWS Marketplace が Amazon マシンイメージ (AMI) をコピーできるようにする AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceAmiIngestion をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 9 月 25 日 20:55 UTC
- 編集日時: 2020 年 9 月 25 日 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMarketplaceDeploymentServiceRolePolicy

AWSMarketplaceDeploymentServiceRolePolicy は、AWS Marketplace でサブスクライブしている商品の出品者デプロイメントパラメータを AWS Marketplace が作成および管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 15 日 23:34 UTC
- 編集日時: 2023 年 11 月 15 日 23:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
```

```
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMarketplaceFullAccess

AWSMarketplaceFullAccess は、AWS Marketplace ソフトウェアの購読・購読解除を可能にし、ユーザーが Marketplace の「あなたのソフトウェア」ページから Marketplace ソフトウェアのインスタンスを管理を可能にし、EC2 への管理者アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 11 日 17:21 UTC
- 編集日時: 2022 年 3 月 4 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMarketplaceGetEntitlements

`AWSMarketplaceGetEntitlements` は、AWS Marketplace エンタイトルメントへの読み取りアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMarketplaceGetEntitlements` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 3 月 27 日 19:37 UTC
- 編集日時: 2017 年 3 月 27 日 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:GetEntitlements"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMarketplaceImageBuildFullAccess

AWSMarketplaceImageBuildFullAccess は、AWS Marketplace Private Image Build 機能へのフルアクセスを提供する AWS マネージドポリシーです。プライベートイメージを作成することに加えて、イメージにタグを追加したり、EC2 インスタンスを起動および終了したりする許可も付与されます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceImageBuildFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 7 月 31 日 23:29 UTC
- 編集日時: 2022 年 3 月 4 日 17:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMarketplaceLicenseManagementServiceRolePolicy

AWSMarketplaceLicenseManagementServiceRolePolicy は、ライセンス管理のために AWS Marketplace が使用または管理している AWS のサービス およびリソースへのアクセスをできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 3 日 08:33 UTC
- 編集日時: 2020 年 12 月 3 日 08:33 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMarketplaceManageSubscriptions

AWSMarketplaceManageSubscriptions は、AWS Marketplace ソフトウェアの購読・購読解除をできるようにする AWS マネージドポリシーです

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceManageSubscriptions をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2023 年 1 月 19 日 23:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMarketplaceMeteringFullAccess

AWSMarketplaceMeteringFullAccess は、AWS Marketplace Metering へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceMeteringFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 3 月 17 日 22:39 UTC
- 編集日時: 2016 年 3 月 17 日 22:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    {
      "Action" : [
        "aws-marketplace:MeterUsage"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMarketplaceMeteringRegisterUsage

AWSMarketplaceMeteringRegisterUsage は、AWS Marketplace Metering Service を通じてリソースを登録し、使用状況を追跡するための許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceMeteringRegisterUsage をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 11 月 21 日 01:17 UTC
- 編集日時: 2019 年 11 月 21 日 01:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMarketplaceProcurementSystemAdminFullAccess

`AWSMarketplaceProcurementSystemAdminFullAccess` は、AWS Marketplace eProcurement インテグレーションのすべての管理者アクションに対してフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMarketplaceProcurementSystemAdminFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 6 月 25 日 13:07 UTC
- 編集日時: 2019 年 6 月 25 日 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMarketplacePurchaseOrdersServiceRolePolicy

AWSMarketplacePurchaseOrdersServiceRolePolicy は、発注書管理の AWS Marketplace サービスへのアクセスをできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 10 月 27 日 15:12 UTC
- 編集日時: 2021 年 10 月 27 日 15:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMarketplaceRead-only

`AWSMarketplaceRead-only` は、AWS Marketplace サブスクリプションを評価できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMarketplaceRead-only` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2023 年 1 月 19 日 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceRead-only`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMarketplaceResaleAuthorizationServiceRolePolicy

`AWSMarketplaceResaleAuthorizationServiceRolePolicy` は、再販売承認 AWS Marketplace のために が使用または管理する AWS のサービス およびリソースへのアクセスを有効にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成時刻: 2024 年 3 月 5 日 18:47 UTC
- 編集日時： 2024 年 3 月 5 日 18:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSMarketplaceSellerFullAccess

`AWSMarketplaceSellerFullAccess` は、 AWS Marketplace および AMI 管理などの他の AWS のサービスに対するすべての販売者オペレーションへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMarketplaceSellerFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 7 月 2 日 20:40 UTC
- 編集日時： 2024 年 3 月 15 日 16:09 UTC

- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSMarketplaceSellerProductsFullAccess

`AWSMarketplaceSellerProductsFullAccess` は、出品者に AWS Marketplace Management Product ページおよび他の AWS サービス (AMI 管理など) へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceSellerProductsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 7 月 2 日 21:06 UTC
- 編集日時: 2023 年 7 月 18 日 22:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMarketplaceSellerProductsReadOnly

AWSMarketplaceSellerProductsReadOnly は、出品者に [AWS Marketplace 管理商品] ページへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceSellerProductsReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 7 月 2 日 21:40 UTC
- 編集日時: 2022 年 11 月 19 日 00:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMediaConnectServicePolicy

AWSMediaConnectServicePolicy は、MediaConnect が使用または管理する AWS のサービス およびリソースへのアクセスをできるようにするデフォルトのポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 4 月 3 日 22:11 UTC
- 編集日時: 2023 年 4 月 3 日 22:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  ]
```

```
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMediaTailorServiceRolePolicy

AWSMediaTailorServiceRolePolicy は、MediaTailor が使用または管理する AWS リソースへのアクセスをできるようにする AWS マネージドポリシーです

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 9 月 17 日 22:27 UTC
- 編集日時: 2021 年 9 月 17 日 22:27 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "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/*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMigrationHubDiscoveryAccess

`AWSMigrationHubDiscoveryAccess` は、AWSMigrationHubService がユーザーに代わって AWSApplicationDiscoveryService を呼び出せるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMigrationHubDiscoveryAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 8 月 14 日 13:30 UTC
- 編集日時: 2020 年 8 月 6 日 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMigrationHubDMSAccess

AWSMigrationHubDMSAccess は Database Migration Service のポリシーであり、顧客のアカウントのロールを引き受けて Migration Hub を呼び出す AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubDMSAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 8 月 14 日 14:00 UTC
- 編集日時: 2019 年 10 月 7 日 17:51 UTC

- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMigrationHubFullAccess

AWSMigrationHubFullAccess は、お客様に Migration Hub Service へのアクセスを提供する AWS マネージドポリシーです

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 8 月 14 日 14:02 UTC
- 編集日時: 2019 年 6 月 19 日 21:14 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMigrationHubOrchestratorConsoleFullAccess

`AWSMigrationHubOrchestratorConsoleFullAccess` は、AWS Migration Hub、AWS Application Discovery Service、Amazon Simple Storage Service、AWS Secrets Manager への制限付きアクセスを提供する AWS マネージドポリシーです。このポリシーでは、AWS Migration Hub Orchestrator サービスへのフルアクセスも付与されます。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMigrationHubOrchestratorConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 4 月 20 日 02:26 UTC
- 編集時間:2023 年 12 月 5 日 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMigrationHubOrchestratorInstanceRolePolicy

AWSMigrationHubOrchestratorInstanceRolePolicy は、S3 からスクリプトをダウンロードしてインスタンスをオーケストレーションしたり、EC2 インスタンス内のシークレット値を取得したりするために、SAP および MGN に移行したインスタンスにアタッチする必要がある AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubOrchestratorInstanceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 4 月 20 日 02:43 UTC
- 編集日時: 2022 年 4 月 20 日 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMigrationHubOrchestratorPlugin

AWSMigrationHubOrchestratorPlugin は、AWS Migration Hub オーケストレーターの Amazon Simple Storage Service、AWS Secrets Manager、プラグイン関連のアクションへの制限付きアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubOrchestratorPlugin をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 4 月 20 日 02:25 UTC
- 編集日時: 2022 年 4 月 20 日 02:25 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
```

```
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMigrationHubOrchestratorServiceRolePolicy

AWSMigrationHubOrchestratorServiceRolePolicy は、Migration Hub オーケストレーターがオンプレミスのワークロードを移行とモダナイズするために必要な許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 4 月 20 日 02:24 UTC
- 編集日時： 2024 年 3 月 4 日 18:25 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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-*"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess は、ネットワークブリッジのない環境を使用するときに必要のない AWS Transit Gateway および EC2 セキュリティグループを除き、AWS Migration Hub リファクタリングスペースおよびその他の AWS 関連サービスへのフルアクセスを付与する AWS マネージドポリシーです。このポリシーでは、タグに基づいてスコープダウンできるため、AWS Lambda および AWS Resource Access Manager に必要な許可も除外されます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 4 月 3 日 20:09 UTC
- 編集日時: 2023 年 7 月 20 日 15:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

`AWSMigrationHubRefactorSpaces-SSMAutomationPolicy` は、オートメーションの実行に必要な許可を付与するため、SSM オートメーションドキュメントの AWSRefactorSpaces-CreateResources に渡された IAM サービスロールを使用する AWS マネージドポリシーです。このポリシーは、自動化の進行状況を追跡するために EC2 タグへの読み取り/書き込みアクセスを許可します。Refactor Spaces 環境のネットワークブリッジが有効になっている場合、環境内の他の Refactor Spaces サービスによるトラフィックを許可するため、オートメーションは環境のセキュリティグループを EC2 インスタンスにも追加します。このポリシーでは、Application Migration Service の起動後アクション SSM パラメータへのアクセスも付与されます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubRefactorSpaces-SSMAutomationPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 8 月 10 日 15:08 UTC
- 編集日時: 2023 年 8 月 10 日 15:08 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-
*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMigrationHubRefactorSpacesFullAccess

AWSMigrationHubRefactorSpacesFullAccess は、AWS MigrationHub リファクタリングスペース、AWS MigrationHub リファクタリングスペースコンソール機能、その他の関連 AWS サービスへのフルアクセスを付与する AWS マネージドポリシーです。ただし、タグに基づいて範囲を絞り込むことが可能であるため、AWS Lambda および AWS Resource Access Manager の必要な許可は除きます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubRefactorSpacesFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 11 月 29 日 07:12 UTC
- 編集日時: 2023 年 7 月 19 日 19:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMigrationHubRefactorSpacesServiceRolePolicy

AWSMigrationHubRefactorSpacesServiceRolePolicy は、AWS Migration Hub リファクタリングスペースが管理または使用する AWS リソースへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 29 日 06:50 UTC
- 編集日時: 2023 年 7 月 20 日 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMigrationHubSMSAccess

AWSMigrationHubSMSAccess は、Server Migration Service のポリシーであり、顧客アカウントのロールを引き受けて Migration Hub を呼び出す AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubSMSAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 8 月 14 日 13:57 UTC
- 編集日時: 2019 年 10 月 7 日 18:01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMigrationHubStrategyCollector

`AWSMigrationHubStrategyCollector` は、AWS Migration Hub Strategy Recommendations サービスとの通信をできるようにする許可、サービスに関連する S3 バケットへの読み取り/書き込みアクセス、ログおよびメトリクスを AWS にアップロードするための Amazon API Gateway アクセス、認証情報を取得するための AWS Secrets Manager アクセス、その他の関連サービスに許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMigrationHubStrategyCollector` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 10 月 19 日 20:15 UTC
- 編集日時： 2024 年 2 月 5 日 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
```

```
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMigrationHubStrategyConsoleFullAccess

`AWSMigrationHubStrategyConsoleFullAccess` は、AWS Migration Hub Strategy Recommendations サービスへのフルアクセスを付与し、AWS Management Console を通じて関連 AWS サービスへのアクセスを付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMigrationHubStrategyConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 10 月 19 日 20:13 UTC
- 編集日時: 2022 年 11 月 9 日 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMigrationHubStrategyServiceRolePolicy

AWSMigrationHubStrategyServiceRolePolicy は、AWS Migration Hub Strategy Recommendations サービスが使用または管理する AWS リソースへのアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 10 月 19 日 20:02 UTC
- 編集日時: 2021 年 10 月 19 日 20:02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMobileHub_FullAccess

AWSMobileHub_FullAccess は、AWS Mobile Hub でプロジェクト (および関連する AWS リソース) を作成、削除、変更する許可をユーザーに付与するため、このポリシーを任意のユーザー、ロール、グループにアタッチできることを記述する AWS マネージドポリシーです。これには、各 Mobile Hub プロジェクトのサンプルモバイルアプリのソースコードを生成およびダウンロードする許可も含まれます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMobileHub_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 1 月 5 日 19:56 UTC
- 編集日時: 2019 年 12 月 19 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSMobileHub_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMobileHub_ReadOnly

AWSMobileHub_ReadOnly は、AWS Mobile Hub でプロジェクトを一覧表示および表示する許可をユーザーに付与するため、任意のユーザー、ロール、グループにアタッチできる AWS マネージドポリシーです。これには、各 Mobile Hub プロジェクトのサンプルモバイルアプリのソースコードを生成およびダウンロードする許可も含まれます。ユーザーは Mobile Hub プロジェクトの設定を変更することはできません。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMobileHub_ReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 1 月 5 日 19:55 UTC
- 編集日時: 2018 年 7 月 23 日 21:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "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"
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSMSKReplicatorExecutionRole

`AWSMSKReplicatorExecutionRole`は、MSK クラスター間でデータをレプリケートするアクセス権限を Amazon MSK Replicator AWSに付与する管理ポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMSKReplicatorExecutionRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成時間:2023 年 12 月 6 日 00:07 UTC
- 編集時間:2023 年 12 月 6 日 00:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*/*"
      ]
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSNetworkFirewallServiceRolePolicy

AWSNetworkFirewallServiceRolePolicy は、AWSNetworkFirewall がファイアウォールに必要なリソースの作成および管理をできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 17 日 17:17 UTC
- 編集日時: 2023 年 3 月 30 日 17:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSNetworkManagerCloudWANServiceRolePolicy

AWSNetworkManagerCloudWANServiceRolePolicy は、NetworkManager が Core Network に関連するリソースにアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 7 月 12 日 12:17 UTC
- 編集日時: 2022 年 7 月 12 日 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSNetworkManagerFullAccess

AWSNetworkManagerFullAccess は、AWS Management Console 経由で Amazon NetworkManager へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSNetworkManagerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 3 日 17:37 UTC
- 編集日時: 2019 年 12 月 3 日 17:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "networkmanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSNetworkManagerReadOnlyAccess

`AWSNetworkManagerReadOnlyAccess` は、AWS Management Console 経由で Amazon NetworkManager への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSNetworkManagerReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 3 日 17:35 UTC
- 編集日時: 2019 年 12 月 3 日 17:35 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSNetworkManagerServiceRolePolicy

`AWSNetworkManagerServiceRolePolicy` は、NetworkManager が Global Networks に関連するリソースへのアクセスをできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 3 日 14:03 UTC
- 編集日時: 2022 年 7 月 27 日 19:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSOpsWorks_FullAccess

AWSOpsWorks_FullAccess は、AWS OpsWorks へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOpsWorks_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2021 年 1 月 22 日 16:29 UTC
- 編集日時: 2021 年 1 月 22 日 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorks_FullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSOpsWorksCloudWatchLogs

AWSOpsWorksCloudWatchLogs は、CWLogs 統合が有効になっている OpsWorks インスタンスがログを送信し、必要なロググループを作成できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOpsWorksCloudWatchLogs をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 3 月 30 日 17:47 UTC
- 編集日時: 2017 年 3 月 30 日 17:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksCloudWatchLogs

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSOpsWorksCMInstanceProfileRole

`AWSOpsWorksCMInstanceProfileRole` は、OpsWorks CM が起動したインスタンスに S3 アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOpsWorksCMInstanceProfileRole をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 11 月 24 日 09:48 UTC
- 編集日時: 2021 年 4 月 23 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksCMInstanceProfileRole

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSOpsWorksCMServiceRole

AWSOpsWorksCMServiceRole は、OpsWorks CM サーバーの作成に使用されるサービスロールポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOpsWorksCMServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2016 年 11 月 24 日 09:49 UTC
- 編集日時: 2021 年 4 月 23 日 17:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSOpsWorksCMServiceRole

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSOpsWorksInstanceRegistration

AWSOpsWorksInstanceRegistration は、Amazon EC2 インスタンスが AWS OpsWorks スタックに登録するためのアクセスを提供する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOpsWorksInstanceRegistration をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 6 月 3 日 14:23 UTC

- 編集日時: 2016 年 6 月 3 日 14:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSOpsWorksRegisterCLI_EC2

AWSOpsWorksRegisterCLI_EC2 は、OpsWorks CLI 経由で EC2 インスタンスの登録をできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOpsWorksRegisterCLI_EC2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 6 月 18 日 15:56 UTC
- 編集日時: 2019 年 6 月 18 日 15:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_EC2

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSOpsWorksRegisterCLI_OnPremises

AWSOpsWorksRegisterCLI_OnPremises は、OpsWorks CLI 経由でオンプレミスインスタンスの登録をできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOpsWorksRegisterCLI_OnPremises をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 6 月 18 日 15:33 UTC

- 編集日時: 2019 年 6 月 18 日 15:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_OnPremises

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSOrganizationsFullAccess

AWSOrganizationsFullAccess は、 AWS Organizations へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOrganizationsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 6 日 20:31 UTC
- 編集日時： 2024 年 2 月 6 日 17:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSOrganizationsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSOrganizationsReadOnlyAccess

`AWSOrganizationsReadOnlyAccess` は、 AWS Organizations への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSOrganizationsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 6 日 20:32 UTC
- 編集日時： 2024 年 2 月 6 日 17:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
```

```
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSOrganizationsServiceTrustPolicy

`AWSOrganizationsServiceTrustPolicy` は、顧客の構成を簡素化する目的として、AWS Organizations が他の承認された AWS のサービス と信頼を共有できるようにする AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 10 日 23:04 UTC
- 編集日時: 2017 年 11 月 1 日 06:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSOutpostsAuthorizeServerPolicy

AWSOutpostsAuthorizeServerPolicy は、Outpost サーバーをオンプレミスネットワークにインストールする許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOutpostsAuthorizeServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 1 月 4 日 19:23 UTC
- 編集日時: 2023 年 1 月 4 日 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSOutpostsServiceRolePolicy

AWSOutpostsServiceRolePolicy は、AWS Outposts が管理する AWS リソースへのアクセスを有効にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 9 日 22:55 UTC
- 編集日時: 2020 年 11 月 9 日 22:55 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSPanoramaApplianceRolePolicy

AWSPanoramaApplianceRolePolicy は、AWS Panorama アプライアンス上の AWS IoT ソフトウェアが Amazon CloudWatch にログをアップロードできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPanoramaApplianceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 1 日 13:13 UTC
- 編集日時: 2020 年 12 月 1 日 13:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSPanoramaApplianceServiceRolePolicy

`AWSPanoramaApplianceServiceRolePolicy` は、AWS Panorama アプライアンスが Amazon CloudWatch にログをアップロードし、AWS Panorama で使用するために作成された Amazon S3 Access Points からオブジェクトを取得できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPanoramaApplianceServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 10 月 20 日 12:14 UTC
- 編集日時: 2023 年 1 月 17 日 21:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSPanoramaFullAccess

AWSPanoramaFullAccess は、AWS Panorama へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPanoramaFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 1 日 13:12 UTC
- 編集日時: 2022 年 1 月 12 日 21:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSPanoramaFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSPanoramaGreengrassGroupRolePolicy

AWSPanoramaGreengrassGroupRolePolicy は、AWS Panorama アプライアンス上の AWS Lambda 関数が Panorama のリソースを管理し、Amazon CloudWatch にログおよびメトリクスをアップロードし、Panorama で使用するために作成されたバケット内のオブジェクトを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPanoramaGreengrassGroupRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 1 日 13:10 UTC
- 編集日時: 2021 年 1 月 6 日 19:30 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSPanoramaSageMakerRolePolicy

AWSPanoramaSageMakerRolePolicy は、Amazon SageMaker が AWS Panorama で使用するために作成されたバケット内のオブジェクトを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPanoramaSageMakerRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2020 年 12 月 1 日 13:13 UTC
- 編集日時: 2020 年 12 月 1 日 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSPanoramaServiceLinkedRolePolicy

AWSPanoramaServiceLinkedRolePolicy は、AWS Panorama が AWS IoT、AWS Secrets Manager、AWS Panorama のリソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 10 月 20 日 12:12 UTC
- 編集日時: 2021 年 10 月 20 日 12:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSPanoramaServiceRolePolicy

AWSPanoramaServiceRolePolicy は、AWS Panorama が Amazon S3、AWS IoT、AWS IoT GreenGrass、AWS Lambda、Amazon SageMaker、Amazon CloudWatch Logs のリソースを管理し、サービスロールを AWS IoT、AWS IoT GreenGrass、Amazon SageMaker に渡せるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPanoramaServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 1 日 13:14 UTC
- 編集日時: 2020 年 12 月 1 日 13:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSPriceListServiceFullAccess

AWSPriceListServiceFullAccess は、AWS 価格表サービスへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPriceListServiceFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 22 日 00:36 UTC
- 編集日時: 2017 年 11 月 22 日 00:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSPrivateCAAuditor

`AWSPrivateCAAuditor` は、監査人に AWS Private Certificate Authority へのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSPrivateCAAuditor` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 2 月 14 日 18:33 UTC
- 編集日時: 2023 年 2 月 14 日 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAAuditor`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSPrivateCAFullAccess

AWSPrivateCAFullAccess は、AWS Private Certificate Authority へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPrivateCAFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 2 月 14 日 18:20 UTC
- 編集日時: 2023 年 2 月 14 日 18:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSPrivateCAPrivilegedUser

AWSPrivateCAPrivilegedUser は、特権証明書ユーザーに AWS Private Certifcate Authority へのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPrivateCAPrivilegedUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 2 月 14 日 18:26 UTC
- 編集日時: 2023 年 2 月 14 日 18:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAPrivilegedUser

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSPrivateCAReadOnly

`AWSPrivateCAReadOnly` は、AWS Private Certificate Authority への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSPrivateCAReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 2 月 14 日 18:30 UTC
- 編集日時: 2023 年 2 月 14 日 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
  }
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSPrivateCAUser

AWSPrivateCAUser は、証明書ユーザーに AWS Private Certificate Authority へのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPrivateCAUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 2 月 14 日 18:16 UTC
- 編集日時: 2023 年 2 月 14 日 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAUser

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSPrivateMarketplaceAdminFullAccess

`AWSPrivateMarketplaceAdminFullAccess` は、 AWS Private Marketplace のすべての管理アクションへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSPrivateMarketplaceAdminFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 27 日 16:32 UTC
- 編集日時： 2024 年 2 月 14 日 22:05 UTC

- ARN: arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSPrivateMarketplaceRequests

`AWSPrivateMarketplaceRequests` は、AWS Private Marketplace でリクエスト作成へのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPrivateMarketplaceRequests をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 10 月 28 日 21:44 UTC
- 編集日時: 2019 年 10 月 28 日 21:44 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSPrivateNetworksServiceRolePolicy

AWSPrivateNetworksServiceRolePolicy は、AWS プライベートネットワークサービスが顧客に代わってリソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 12 月 16 日 23:17 UTC
- 編集日時: 2021 年 12 月 16 日 23:17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSProtonCodeBuildProvisioningBasicAccess

AWSProtonCodeBuildProvisioningBasicAccess は、CodeBuild が AWS Proton CodeBuild プロビジョニングのビルドを実行するために必要な許可である AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSProtonCodeBuildProvisioningBasicAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 9 日 21:04 UTC
- 編集日時: 2022 年 11 月 9 日 21:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*:*:*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSProtonCodeBuildProvisioningServiceRolePolicy

AWSProtonCodeBuildProvisioningServiceRolePolicy は、AWS Proton がユーザーに代わって CodeBuild およびその他の AWS サービスを使用して Proton リソースのプロビジョニングを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 9 日 21:32 UTC
- 編集日時: 2023 年 5 月 17 日 16:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSProtonDeveloperAccess

AWSProtonDeveloperAccess は、AWS Proton API および Management Console へのアクセスを提供しますが、Proton テンプレートや環境の管理を許可しない AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSProtonDeveloperAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 2 月 17 日 19:02 UTC
- 編集日時: 2022 年 11 月 18 日 18:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonDeveloperAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSProtonFullAccess

`AWSProtonFullAccess` は、AWS Proton API および Management Console へのフルアクセスを提供する AWS マネージドポリシーです。これらの許可に加えて、S3 バケットからテンプレートバン

ドルを登録するには Amazon S3 へのアクセスも必要です。また、Proton のサービスロールを作成および管理するための Amazon IAM へのアクセスも必要です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSProtonFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 2 月 17 日 19:07 UTC
- 編集日時: 2022 年 6 月 20 日 12:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
```

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSProtonReadOnlyAccess

`AWSProtonReadOnlyAccess` は、AWS Proton API および Management Console への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSProtonReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 2 月 17 日 19:09 UTC
- 編集日時: 2022 年 11 月 18 日 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSProtonServiceGitSyncServiceRolePolicy

AWSProtonServiceGitSyncServiceRolePolicy は、AWS Proton が git リポジトリのサービス、環境、コンポーネントの定義を AWS Proton に同期できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 4 月 4 日 15:55 UTC
- 編集日時: 2023 年 4 月 4 日 15:55 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSProtonSyncServiceRolePolicy

AWSProtonSyncServiceRolePolicy は、AWS Proton が git リポジトリの内容を Proton に同期または Proton の内容を git リポジトリに同期できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 23 日 21:14 UTC
- 編集日時: 2021 年 11 月 23 日 21:14 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSPurchaseOrdersServiceRolePolicy

AWSPurchaseOrdersServiceRolePolicy は、請求コンソールで注文書を表示および変更する許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPurchaseOrdersServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 5 月 6 日 18:15 UTC
- 編集日時: 2023 年 7 月 17 日 18:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSQuicksightAthenaAccess

AWSQuicksightAthenaAccess は、Athena のクエリ結果に使用される Athena API および S3 バケットへの Quicksight アクセスに関する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuicksightAthenaAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 12 月 9 日 02:31 UTC
- 編集日時: 2021 年 7 月 7 日 20:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSQuickSightDescribeRDS

AWSQuickSightDescribeRDS は、QuickSight が RDS リソースを記述できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightDescribeRDS をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 11 月 10 日 23:24 UTC
- 編集日時: 2015 年 11 月 10 日 23:24 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSQuickSightDescribeRedshift

`AWSQuickSightDescribeRedshift` は、QuickSight が Redshift リソースを記述できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSQuickSightDescribeRedshift` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 11 月 10 日 23:25 UTC
- 編集日時: 2015 年 11 月 10 日 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSQuickSightElasticsearchPolicy

AWSQuickSightElasticsearchPolicy は、Amazon QuickSight から Amazon Elasticsearch リソースへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightElasticsearchPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 9 月 9 日 17:27 UTC
- 編集日時: 2021 年 9 月 7 日 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSQuickSightIoTAnalyticsAccess

AWSQuickSightIoTAnalyticsAccess は、QuickSight に IoT Analytics データセットへの読み取り専用アクセスを付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightIoTAnalyticsAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 29 日 17:00 UTC
- 編集日時: 2017 年 11 月 29 日 17:00 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSQuickSightListIAM

AWSQuickSightListIAM は、QuickSight が IAM エンティティを一覧表示できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightListIAM をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 11 月 10 日 23:25 UTC
- 編集日時: 2015 年 11 月 10 日 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSQuicksightOpenSearchPolicy

AWSQuicksightOpenSearchPolicy は、Amazon QuickSight から Amazon OpenSearch リソースへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuicksightOpenSearchPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 9 月 7 日 23:26 UTC
- 編集日時: 2021 年 9 月 7 日 23:26 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
```

```
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSQuickSightSageMakerPolicy

`AWSQuickSightSageMakerPolicy` は、Amazon QuickSight から Amazon SageMaker のリソースへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSQuickSightSageMakerPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 1 月 17 日 17:18 UTC
- 編集日時: 2023 年 10 月 30 日 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSQuickSightTimestreamPolicy

AWSQuickSightTimestreamPolicy は、AWS Timestream API への AWS QuickSight アクセスである AWS マネージドポリシー です。顧客はこのポリシーを AWS QuickSight ロールにアタッチし、データおよびメタデータの取得を許可できます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightTimestreamPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 9 月 30 日 21:47 UTC
- 編集日時: 2020 年 9 月 30 日 21:47 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSReachabilityAnalyzerServiceRolePolicy

`AWSReachabilityAnalyzerServiceRolePolicy`は、VPC Reachability Analyzer がユーザーに代わって AWS リソースにアクセスし、AWS Organizations と統合できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 23 日 17:12 UTC
- 編集日時: 2023 年 6 月 23 日 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSRefactoringToolkitFullAccess

AWSRefactoringToolkitFullAccess は、Microsoft Visual Studio の AWS Toolkit for .NET リファクタリング拡張機能で AWS サービスを使用する許可を付与する AWS マネージドポリシーです。ローカル AWS プロファイルにアタッチすることを目的としています。このポリシーにより、アプリケーションアーティファクトのアップロードし、Amazon S3 からの結果のアーティファクトをダウンロードできます。これにより、Amazon Elastic Container Registry (Amazon ECR) からイメージを使用し、AWS CodeBuild 保存および取得するアプリケーションをコンテナイメージに組み込むことができます。また、Amazon Elastic Container Service (Amazon ECS) など、AWSでコンテナサービスへのアプリケーションのデプロイ、VPC リソースのオプション作成、AWS Directory Service などの既存インフラストラクチャへのオプション接続、その他の関連サービスが可能になります。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSRefactoringToolkitFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 10 月 25 日 16:41 UTC
- 編集時間:2023 年 11 月 18 日 00:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSRefactoringToolkitSidecarPolicy

AWSRefactoringToolkitSidecarPolicy は、Microsoft Visual Studio の AWS Toolkit for .NET リファクタリング拡張機能を使用して AWS のアプリケーションをテストするために作成された Amazon ECS タスクによって使用されることを目的とする AWS マネージドポリシーです。このポリシーは、Amazon S3 からアプリケーションアーティファクトをダウンロード、AWS Systems Manager を使用してタスクのステータスの通信、その他の必要なサービスのアクセスを許可します。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSRefactoringToolkitSidecarPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 10 月 25 日 16:41 UTC
- 編集日時: 2022 年 10 月 29 日 22:15 UTC

- ARN: arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSrePostPrivateCloudWatchAccess

`AWSrePostPrivateCloudWatchAccess`は、AWS次のような管理ポリシーです。 CloudWatch メトリクスデータを公開するための re: Post Private アクセスを提供します。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 15 日 16:37 UTC
- 編集日時: 2023 年 11 月 15 日 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSRepostSpaceSupportOperationsPolicy

AWSRepostSpaceSupportOperationsPolicyAWSは次のような管理ポリシーです。このポリシーにより、re: Post Space サービスは Space アプリケーションを通じて作成されたSupport ケースを作成、管理、および解決できます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSRepostSpaceSupportOperationsPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時間:2023 年 11 月 26 日 21:52 UTC
- 編集時間:2023 年 11 月 26 日 21:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSResilienceHubAsssessmentExecutionPolicy

AWSResilienceHubAsssessmentExecutionPolicy は、評価を実行するために他の AWS サービスへのアクセスを許可する AWS Resilience Hub サービスロール用の AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSResilienceHubAsssessmentExecutionPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 6 月 27 日 12:32 UTC
- 編集日時: 2023 年 10 月 29 日 16:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSResourceAccessManagerFullAccess

AWSResourceAccessManagerFullAccess は、AWS Resource Access Manager へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSResourceAccessManagerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 6 月 4 日 17:28 UTC
- 編集日時: 2019 年 6 月 4 日 17:28 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSResourceAccessManagerReadOnlyAccess

AWSResourceAccessManagerReadOnlyAccess は、AWS Resource Access Manager への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSResourceAccessManagerReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 9 日 20:58 UTC
- 編集日時: 2019 年 12 月 9 日 20:58 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSResourceAccessManagerResourceShareParticipantAccess

AWSResourceAccessManagerResourceShareParticipantAccess は、リソース共有参加者が必要とする AWS Resource Access Manager API へのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSResourceAccessManagerResourceShareParticipantAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 9 日 20:41 UTC

- 編集日時: 2019 年 12 月 9 日 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSResourceAccessManagerServiceRolePolicy

AWSResourceAccessManagerServiceRolePolicy は、AWS Resource Access Manager が顧客の Organizations 構造への読み取り専用アクセスを含む AWS マネージドポリシーです。ロールを自己削除するための IAM アクセス許可も含まれます。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 14 日 19:28 UTC
- 編集日時: 2018 年 11 月 14 日 19:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSResourceExplorerFullAccess

AWSResourceExplorerFullAccess は、このポリシーは、Resource Explorer リソースにアクセスするための管理許可を付与し、このアクセスをサポートするために他の AWS サービスに読み取り専用許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSResourceExplorerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 7 日 20:01 UTC
- 編集日時: 2023 年 11 月 14 日 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSResourceExplorerOrganizationsAccess

`AWSResourceExplorerOrganizationsAccess` は、Resource Explorer に管理許可を付与し、このアクセスをサポートするために他の AWS サービスに読み取り専用許可を付与する AWS マネージドポリシーです。AWS Organizations 管理者がコンソールでマルチアカウント検索を設定して管理するには、これらの許可が必要です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSResourceExplorerOrganizationsAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 11 月 14 日 17:01 UTC
- 編集日時: 2023 年 11 月 14 日 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSResourceExplorerReadOnlyAccess

AWSResourceExplorerReadOnlyAccess は、Resource Explorer リソースを検索および表示するための読み取り専用許可を付与し、このアクセスをサポートするために他の AWS サービスには読み取り専用許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSResourceExplorerReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 7 日 19:56 UTC
- 編集日時: 2023 年 11 月 14 日 16:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSResourceExplorerServiceRolePolicy

AWSResourceExplorerServiceRolePolicyは、 CloudTrail リソースエクスプローラーがユーザーに代わってリソースとイベントを表示し、AWS検索用のリソースにインデックスを付けることを許可する管理ポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 10 月 25 日 20:35 UTC
- 編集時間:2023 年 12 月 20 日 13:58 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSResourceGroupsReadOnlyAccess

AWSResourceGroupsReadOnlyAccess は、AWS Resource Groups の読み取り専用の AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSResourceGroupsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 3 月 7 日 10:27 UTC
- 編集日時: 2019 年 2 月 5 日 17:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSRoboMaker_FullAccess

`AWSRoboMaker_FullAccess` は、AWS Management Console および SDK 経由で AWS RoboMaker へのフルアクセスを提供する AWS マネージドポリシーです。関連サービス (S3 や IAM など) への限定アクセスも提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSRoboMaker_FullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2020 年 9 月 10 日 18:34 UTC
- 編集日時: 2021 年 9 月 16 日 21:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSRoboMakerReadOnlyAccess

`AWSRoboMakerReadOnlyAccess` は、AWS Management Console および SDK 経由で AWS RoboMaker への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSRoboMakerReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 26 日 05:30 UTC
- 編集日時: 2020 年 8 月 28 日 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSRoboMakerServicePolicy

AWSRoboMakerServicePolicy は、RoboMaker サービスポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 26 日 06:30 UTC
- 編集日時: 2021 年 11 月 11 日 22:23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSRoboMakerServiceRolePolicy

AWSRoboMakerServiceRolePolicy は、RoboMaker サービスポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSRoboMakerServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 26 日 05:33 UTC
- 編集日時: 2018 年 11 月 26 日 05:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSRolesAnywhereServicePolicy

`AWSRolesAnywhereServicePolicy` は、IAM Roles Anywhere がユーザーに代わって CloudWatch にサービス/使用状況のメトリクスを公開し、Private Certificate Authorities のステータスを確認できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 7 月 5 日 15:26 UTC
- 編集日時: 2022 年 7 月 5 日 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*:*:*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSS3OnOutpostsServiceRolePolicy

AWSS3OnOutpostsServiceRolePolicy は、Amazon S3 on Outposts サービスがユーザーに代わって EC2 ネットワークリソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 10 月 3 日 20:32 UTC
- 編集日時: 2023 年 10 月 3 日 20:32 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSavingsPlansFullAccess

`AWSSavingsPlansFullAccess` は、Savings Plans サービスへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSavingsPlansFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 11 月 6 日 22:45 UTC
- 編集日時: 2019 年 11 月 6 日 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSavingsPlansReadOnlyAccess

AWSSavingsPlansReadOnlyAccess は、Savings Plans サービスへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSavingsPlansReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 11 月 6 日 22:45 UTC
- 編集日時: 2019 年 11 月 6 日 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSecurityHubFullAccess

AWSSecurityHubFullAccess は、AWS Security Hub を使用するためのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSecurityHubFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 27 日 23:54 UTC
- 編集時間:2023 年 11 月 16 日 21:10 UTC
- ARN: arn:aws:iam::aws:policy/AWSSecurityHubFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSecurityHubOrganizationsAccess

AWSSecurityHubOrganizationsAccess は、組織内の AWS Security Hub を有効化および管理する許可を付与する AWS マネージドポリシーです。組織全体でサービスの有効化およびサービスの委任管理者アカウントの決定が含まれます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSecurityHubOrganizationsAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2021 年 3 月 15 日 20:53 UTC
- 編集時間:2023 年 11 月 16 日 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubOrganizationsAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSecurityHubReadOnlyAccess

`AWSSecurityHubReadOnlyAccess` は、 AWS Security Hub リソースへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSecurityHubReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 28 日 01:34 UTC
- 編集日時： 2024 年 2 月 22 日 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

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

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSSecurityHubServiceRolePolicy

AWSSecurityHubServiceRolePolicy は、AWS Security Hub がリソースにアクセスするために必要なサービスリンクロールである AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 27 日 23:47 UTC
- 編集時間:2023 年 11 月 27 日 03:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceCatalogAdminFullAccess

AWSServiceCatalogAdminFullAccess は、サービスカタログの管理者機能へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSServiceCatalogAdminFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 2 月 15 日 17:19 UTC
- 編集日時: 2023 年 4 月 13 日 18:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceCatalogAdminReadOnlyAccess

`AWSServiceCatalogAdminReadOnlyAccess` は、Service Catalog の管理者機能への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSServiceCatalogAdminReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 10 月 25 日 18:53 UTC
- 編集日時: 2019 年 10 月 25 日 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceCatalogAppRegistryFullAccess

AWSServiceCatalogAppRegistryFullAccessは、Service Catalog App Registry 機能へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSServiceCatalogAppRegistryFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 11 月 12 日 22:25 UTC
- 編集時間:2023 年 12 月 7 日 21:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*:*:*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceCatalogAppRegistryReadOnlyAccess

`AWSServiceCatalogAppRegistryReadOnlyAccess` は、Service Catalog App Registry 機能への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSServiceCatalogAppRegistryReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 11 月 12 日 22:34 UTC
- 編集日時: 2022 年 11 月 17 日 18:16 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceCatalogAppRegistryServiceRolePolicy

AWSServiceCatalogAppRegistryServiceRolePolicy は、Service Catalog AppRegistry がユーザーに代わって Resource Groups を管理できるようにする AWS マネージドポリシー です

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 5 月 18 日 22:18 UTC
- 編集日時: 2022 年 10 月 26 日 16:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceCatalogEndUserFullAccess

AWSServiceCatalogEndUserFullAccess は、サービスカタログのエンドユーザー機能へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSServiceCatalogEndUserFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 2 月 15 日 17:22 UTC
- 編集日時: 2019 年 7 月 10 日 20:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceCatalogEndUserReadOnlyAccess

AWSServiceCatalogEndUserReadOnlyAccess は、Service Catalog のエンドユーザー機能への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSServiceCatalogEndUserReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 10 月 25 日 18:49 UTC
- 編集日時: 2019 年 10 月 25 日 18:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

`AWSServiceCatalogOrgsDataSyncServiceRolePolicy` は、AWS ServiceCatalog が AWS Organizations の組織構造と同期する Service Linked Role Policy に関する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 4 月 10 日 20:48 UTC
- 編集日時: 2023 年 4 月 10 日 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceCatalogSyncServiceRolePolicy

`AWSServiceCatalogSyncServiceRolePolicy` は、AWS ServiceCatalog がソースリポジトリのプロビジョニングアーティファクトと同期する Service Linked Role に関する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 15 日 21:20 UTC
- 編集日時: 2022 年 11 月 15 日 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceRoleForAmazonEKSNodegroup

AWSServiceRoleForAmazonEKSNodegroup は、顧客アカウント内のノードグループの管理に必要な許可を付与する AWS マネージドポリシーです。これらのポリシーは AutoscalingGroups、、SecurityGroups、 LaunchTemplates および リソースの管理に関連しています InstanceProfiles。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2019 年 11 月 7 日 01:34 UTC
- 編集日時： 2024 年 1 月 4 日 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy は、CloudWatch Alarms が使用する Systems Manager リソースへのアクセスを提供する AWSマネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 10 月 1 日 09:49 UTC
- 編集日時: 2020 年 10 月 1 日 09:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePoli

`AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy` は、CloudWatch がユーザーに代わって RDS Performance Insights メトリクスにアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 9 月 7 日 09:32 UTC
- 編集日時: 2023 年 9 月 7 日 09:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceRoleForCodeGuru-Profiler

AWSServiceRoleForCodeGuru-Profiler は、Amazon CodeGuru Profiler がユーザーに代わって通知を送信するために必要なサービスリンクロールに関する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 6 月 26 日 22:04 UTC
- 編集日時: 2020 年 6 月 26 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceRoleForCodeWhispererPolicy

AWSServiceRoleForCodeWhispererPolicy は、アカウントのデータにアクセスして請求額を計算 CodeWhisperer するためのアクセス許可を に付与し、Amazon でセキュリティレポートを作成およびアクセスするためのアクセス許可を付与し CodeGuru、 にデータを発行する AWS マネージドポリシーです CloudWatch。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 3 月 24 日 19:39 UTC
- 編集日時： 2024 年 3 月 1 日 23:35 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForEC2ScheduledInstances

AWSServiceRoleForEC2ScheduledInstances は、EC2 でスケジューリングされたインスタンスがスポットインスタンスの起動と管理をできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 12 日 18:31 UTC
- 編集日時: 2017 年 10 月 12 日 18:31 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicyは、AWS GroundStation がこのサービスリンクロールを使用して EC2 を呼び出し、パブリック IPv4 アドレスを検索することに関する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 12 月 13 日 23:52 UTC
- 編集日時: 2022 年 12 月 13 日 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceRoleForImageBuilder

AWSServiceRoleForImageBuilder は、EC2ImageBuilder がユーザーに代わって AWS サービスを呼び出せるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 29 日 22:02 UTC
- 編集日時: 2023 年 10 月 19 日 21:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder

ポリシーのバージョン

ポリシーのバージョン: v19 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceRoleForIoTSiteWise

AWSServiceRoleForIoTSiteWiseは、AWS IoT SiteWise がゲートウェイのプロビジョニングと管理、AWSおよびデータのクエリを実行できるようにする管理ポリシーです。このポリシーには、グループにデプロイするために必要な AWS Greengrass 許可、サービスプレフィックス付き関数を作成および更新するための AWS Lambda 許可、データストアからデータをクエリするための AWS IoT Analytics 許可が含まれます。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 14 日 19:19 UTC
- 編集日時: 2023 年 11 月 13 日 18:27 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceRoleForLogDeliveryPolicy

AWSServiceRoleForLogDeliveryPolicy は、ログ配信サービスがユーザーに代わってログデスティネーションを呼び出してログを配信できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 10 月 4 日 17:31 UTC

- 編集日時: 2021 年 7 月 15 日 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LogDeliveryEnabled" : "true"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceRoleForMonitronPolicy

AWSServiceRoleForMonitronPolicy は、Amazon Monitron がユーザーに代わって AWS SSO ユーザー割り当てなど、AWS リソースを管理する許可を付与するする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 2 日 19:06 UTC
- 編集日時: 2022 年 9 月 29 日 20:38 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceRoleForNeptuneGraphPolicy

AWSServiceRoleForNeptuneGraphPolicyは、AWS次のような管理ポリシーです。Amazon Neptune の運用および使用状況のメトリクスとログを公開するための Cloudwatch アクセスを提供します。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成時間:2023 年 11 月 29 日 14:03 UTC
- 編集時間:2023 年 11 月 29 日 14:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceRoleForPrivateMarketplaceAdminPolicy

`AWSServiceRoleForPrivateMarketplaceAdminPolicy` は、 Private Marketplace リソースを記述および更新し、 AWS Organizations を記述するアクセス許可を提供する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成時刻: 2024 年 2 月 14 日 22:28 UTC
- 編集日時： 2024 年 2 月 14 日 22:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
```

```
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSServiceRoleForSMS

AWSServiceRoleForSMS は、EC2、S3、Cloudformation を含む AWS へのサービスインスタンスの移行に必要な AWS サービスおよびリソースへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 8 月 6 日 18:39 UTC
- 編集日時: 2020 年 10 月 15 日 17:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceRolePolicyForBackupReports

AWSServiceRolePolicyForBackupReports は、AWS Backup がユーザーに代わってコンプライアンスレポートを作成する許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 8 月 19 日 21:16 UTC
- 編集日時: 2023 年 3 月 10 日 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSServiceRolePolicyForBackupRestoreTesting

AWSServiceRolePolicyForBackupRestoreTesting は、リストアをテストしたり、テスト中に作成されたリソースをクリーンアップしたりする許可が含まれる AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 10 日 23:37 UTC
- 編集日時： 2024 年 2 月 14 日 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSShieldDRTAccessPolicy

AWSShieldDRTAccessPolicy は、重大度の高いイベント発生時に DDoS 攻撃の軽減を支援するため、AWS DDoS レスポンスチームに対してユーザーの AWS アカウント に制限付きアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSShieldDRTAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 6 月 5 日 22:29 UTC
- 編集日時: 2020 年 12 月 15 日 17:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSShieldServiceRolePolicy

`AWSShieldServiceRolePolicy` は、AWS Shield がユーザーに代わって AWS リソースにアクセスし、DDoS 保護を提供できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 17 日 19:17 UTC
- 編集日時: 2021 年 11 月 17 日 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSSMForSAPServiceLinkedRolePolicy

AWSSSMForSAPServiceLinkedRolePolicy は、SAP ソフトウェアを AWS で管理および統合に必要な許可を AWS Systems Manager for SAP に提供する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2022 年 11 月 16 日 01:18 UTC
- 編集時間:2023 年 11 月 21 日 03:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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_*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSSMOpsInsightsServiceRolePolicy

AWSSSMOpsInsightsServiceRolePolicy は、Service Linked Role の AWSServiceRoleForAmazonSSM_OpsInsights 用の AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 6 月 16 日 20:12 UTC
- 編集日時: 2021 年 6 月 16 日 20:12 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSSMOpsInsightsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSSODirectoryAdministrator

AWSSSODirectoryAdministrator は、SSO ディレクトリの管理者アクセスを付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSSODirectoryAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 10 月 31 日 23:54 UTC
- 編集日時: 2022 年 10 月 20 日 20:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSSODirectoryReadOnly

`AWSSSODirectoryReadOnly` は、SSO ディレクトリの ReadOnly アクセスを付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSSODirectoryReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 10 月 31 日 23:49 UTC
- 編集日時: 2022 年 11 月 16 日 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSSOMasterAccountAdministrator

`AWSSSOMasterAccountAdministrator` は、AWS Organizations マスターアカウント、メンバーアカウント、クラウドアプリケーションを管理するために AWS SSO 内のアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSSOMasterAccountAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 6 月 27 日 20:36 UTC
- 編集日時: 2022 年 10 月 20 日 20:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSSOMemberAccountAdministrator

AWSSSOMemberAccountAdministrator は、AWS 組織のメンバーアカウントおよびクラウドアプリケーションを管理するために AWS SSO 内のアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSSOMemberAccountAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 6 月 27 日 20:45 UTC
- 編集日時: 2022 年 10 月 20 日 20:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSSOReadOnly

AWSSSOReadOnly は、AWS SSO 設定への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSSOReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 6 月 27 日 20:24 UTC
- 編集日時: 2022 年 8 月 22 日 17:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOReadOnly

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSSOServiceRolePolicy

`AWSSSOServiceRolePolicy` は、AWS SSO がユーザーの代わりに IAM ロール、ポリシー、SAML IdP などの AWS リソースを管理する許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 12 月 5 日 18:36 UTC
- 編集日時: 2022 年 10 月 20 日 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v17 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSStepFunctionsConsoleFullAccess

AWSStepFunctionsConsoleFullAccess は、ユーザー/ロール/その他に AWS StepFunctions コンソールへのアクセスを提供するアクセスポリシーである AWS マネージドポリシーです。コンソールをフルに活用するには、このポリシーに加えて、ユーザーはサービスが引き受けることが可能な他の IAM ロールに iam:PassRole 許可が必要な場合があります。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSStepFunctionsConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 1 月 11 日 21:54 UTC
- 編集日時: 2017 年 1 月 12 日 00:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSStepFunctionsFullAccess

AWSStepFunctionsFullAccess は、ユーザー/ロール/その他に AWS StepFunctions API へのアクセスを提供するアクセスポリシーである AWS マネージドポリシーです。フルアクセスを得るには、このポリシーに加えて、ユーザーはサービスが引き受けることが可能な IAM ロールを最低 1 つでも iam:PassRole 許可が付与される必要があります。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSStepFunctionsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 1 月 11 日 21:51 UTC
- 編集日時: 2017 年 1 月 11 日 21:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSStepFunctionsReadOnlyAccess

`AWSStepFunctionsReadOnlyAccess` は、AWS StepFunctions サービスにユーザー/ロール/その他の読み取り専用アクセスを提供するアクセスポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSStepFunctionsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 1 月 11 日 21:46 UTC
- 編集日時: 2017 年 11 月 10 日 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSStorageGatewayFullAccess

`AWSStorageGatewayFullAccess` は、AWS Management Console 経由で AWS Storage Gateway へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSStorageGatewayFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC

- 編集日時: 2022 年 9 月 6 日 20:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSStorageGatewayReadOnlyAccess

`AWSStorageGatewayReadOnlyAccess` は、AWS Management Console 経由で AWS Storage Gateway へのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSStorageGatewayReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2022 年 9 月 6 日 20:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSStorageGatewayServiceRolePolicy

`AWSStorageGatewayServiceRolePolicy` は、Storage Gateway と他の AWS サービスを統合できるようにするため、AWS Storage Gateway が使用するサービスリンクロールである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 2 月 17 日 19:03 UTC
- 編集日時: 2021 年 2 月 17 日 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSupplyChainFederationAdminAccess

AWSSupplyChainFederationAdminAccessは、AWSサプライ・チェーン・アプリケーション内でアクションを実行するために必要な権限を含め、AWSAWSAWSサプライ・チェーン・アプリケーションへのアクセス権をサプライ・チェーン・フェデレーテッド・ユーザーに付与する管理ポリシーです。 AWSSupplyChainFederationAdminAccess このポリシーにより、IAM アイデンティティセンターのユーザーおよびグループに管理許可が付与され、ユーザーに代わって AWS サプライチェーンが作成したロールにアタッチされます。 AWSSupplyChainFederationAdminAccess ポリシーを他の IAM エンティティにアタッチしないでください。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSupplyChainFederationAdminAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 3 月 1 日 18:54 UTC
- 編集日時: 2023 年 11 月 1 日 18:50 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSupportAccess

AWSSupportAccess は、ユーザーが AWS Support センターにアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSupportAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSupportAppFullAccess

`AWSSupportAppFullAccess` は、AWS Support アプリおよびその他の必要なサービス (AWS Support や Service Quotas など) にフルアクセスを提供する AWS マネージドポリシーです。このポリシーには、ユーザーがサポートケースについて AWS Support に連絡、Service Quotas の変更、関連するサービスにリンクされたロールの作成できるように、対応するサービスを使用する許可が含まれています。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSupportAppFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 8 月 22 日 16:53 UTC
- 編集日時: 2022 年 8 月 22 日 16:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportAppFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSupportAppReadOnlyAccess

AWSSupportAppReadOnlyAccess は、AWS Support アプリに読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSupportAppReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 8 月 22 日 17:01 UTC
- 編集日時: 2022 年 8 月 22 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSupportPlansFullAccess

AWSSupportPlansFullAccess は、サポートプランへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSupportPlansFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 9 月 27 日 18:19 UTC
- 編集日時: 2023 年 5 月 9 日 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSupportPlansReadOnlyAccess

AWSSupportPlansReadOnlyAccess は、サポートプランへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSupportPlansReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 9 月 27 日 18:08 UTC
- 編集日時: 2022 年 9 月 27 日 18:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSupportServiceRolePolicy

`AWSSupportServiceRolePolicy` は、AWS Supportが AWS リソースにアクセスして請求、管理、サポートサービスを提供できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 4 月 19 日 18:04 UTC
- 編集日時： 2024 年 1 月 17 日 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v34 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSystemsManagerAccountDiscoveryServicePolicy

AWSSystemsManagerAccountDiscoveryServicePolicy は、AWS Systems Manager (SSM) に AWS アカウント 情報を検出する許可を付与するする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 10 月 24 日 17:21 UTC
- 編集日時: 2022 年 10 月 17 日 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSystemsManagerChangeManagementServicePolicy

AWSSystemsManagerChangeManagementServicePolicy は、AWS Systems Manager の変更管理フレームワークが管理または使用する AWS リソースへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 7 日 22:21 UTC
- 編集日時: 2020 年 12 月 7 日 22:21 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSystemsManagerForSAPFullAccess

`AWSSystemsManagerForSAPFullAccess` は、AWS Systems Manager for SAP サービスへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSystemsManagerForSAPFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 17 日 02:11 UTC
- 編集日時: 2022 年 11 月 18 日 21:58 UTC
- ARN: arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSystemsManagerForSAPReadOnlyAccess

`AWSSystemsManagerForSAPReadOnlyAccess` は、SAP サービス用 AWS Systems Manager への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSSystemsManagerForSAPReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 17 日 02:11 UTC
- 編集日時: 2022 年 11 月 17 日 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",
        "ssm-sap:list*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSSystemsManagerOpsDataSyncServiceRolePolicy

`AWSSystemsManagerOpsDataSyncServiceRolePolicy` は、OpsData 関連の運用を管理する SSM Explorer の IAM ロールである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 4 月 26 日 20:42 UTC
- 編集日時: 2023 年 6 月 28 日 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSThinkboxAssetServerPolicy

AWSThinkboxAssetServerPolicy は、AWS Portal Asset Server が通常の運用に必要な許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxAssetServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 5 月 27 日 19:18 UTC
- 編集日時: 2020 年 5 月 27 日 19:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSThinkboxAWSPortalAdminPolicy

AWSThinkboxAWSPortalAdminPolicy は、 AWS Thinkbox の Deadline ソフトウェアに AWS 、ポータル管理に必要な複数の AWS サービスへのフルアクセスを付与する AWS マネージドポリシーです。これには、複数の EC2 リソースタイプに任意のタグを作成するためのアクセス権限が含まれます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxAWSPortalAdminPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 5 月 27 日 19:41 UTC
- 編集日時： 2024 年 2 月 23 日 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSThinkboxAWSPortalGatewayPolicy

AWSThinkboxAWSPortalGatewayPolicy は、AWS Portal Gateway マシンが通常の運用に必要な許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxAWSPortalGatewayPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 5 月 27 日 19:05 UTC
- 編集日時: 2020 年 6 月 30 日 16:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSThinkboxAWSPortalWorkerPolicy

AWSThinkboxAWSPortalWorkerPolicy は、AWS Portal の Deadline Workers が通常の運用に必要な許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxAWSPortalWorkerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 5 月 27 日 19:15 UTC
- 編集日時: 2020 年 12 月 7 日 23:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSThinkboxDeadlineResourceTrackerAccessPolicy

`AWSThinkboxDeadlineResourceTrackerAccessPolicy` は、AWS Thinkbox の Deadline Resource Tracker の運用に必要な許可を付与する AWS マネージドポリシーです。これには、DeleteFleets や CancelSpotFleetRequests など、一部の EC2 アクションへのフルアクセスが含まれます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxDeadlineResourceTrackerAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 5 月 27 日 19:25 UTC
- 編集日時: 2020 年 5 月 27 日 19:25 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSThinkboxDeadlineResourceTrackerAdminPolicy

AWSThinkboxDeadlineResourceTrackerAdminPolicy は、AWS Thinkbox の Deadline Resource Tracker の作成、破棄、管理に必要な許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxDeadlineResourceTrackerAdminPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 5 月 27 日 19:29 UTC
- 編集日時: 2022 年 6 月 22 日 18:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

`AWSThinkboxDeadlineSpotEventPluginAdminPolicy` は、AWS Thinkbox の Deadline Spot Event Plugin に必要な許可を付与する AWS マネージドポリシーです。これには、スポットフリートをリクエスト、変更、キャンセルする許可の他に、制限付きの PassRole 許可が含まれます。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSThinkboxDeadlineSpotEventPluginAdminPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 5 月 27 日 19:38 UTC
- 編集日時: 2020 年 5 月 27 日 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy は、AWS Thinkbox Deadline Spot Event Plugin Worker ソフトウェアを実行している EC2 インスタンスに必要な許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxDeadlineSpotEventPluginWorkerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 5 月 27 日 19:35 UTC
- 編集日時: 2020 年 12 月 7 日 23:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSTransferConsoleFullAccess

`AWSTransferConsoleFullAccess` は、AWS Management Console 経由で AWS Transfer へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSTransferConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 14 日 19:33 UTC
- 編集日時: 2020 年 12 月 14 日 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
```

```
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSTransferFullAccess

`AWSTransferFullAccess` は、AWS Transfer Service へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSTransferFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 14 日 19:37 UTC
- 編集日時: 2020 年 12 月 14 日 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSTransferLoggingAccess

AWSTransferLoggingAccess は、AWS Transfer がログストリームおよびグループを作成し、アカウントにログイベントを記録するためのフルアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSTransferLoggingAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 1 月 14 日 15:32 UTC
- 編集日時: 2019 年 1 月 14 日 15:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSTransferReadOnlyAccess

`AWSTransferReadOnlyAccess` は、AWS Transfer サービスへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSTransferReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 8 月 27 日 17:54 UTC
- 編集日時: 2020 年 8 月 27 日 17:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSTrustedAdvisorPriorityFullAccess

`AWSTrustedAdvisorPriorityFullAccess` は、AWS Trusted Advisor Priority へのフルアクセスを提供する AWS マネージドポリシーです。このポリシーは、ユーザーが AWS Organizations を使用して Trusted Advisor を信頼されたサービスとして追加し、Trusted Advisor Priority に委任管理者アカウントを指定できるようにします。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSTrustedAdvisorPriorityFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 8 月 16 日 16:08 UTC

- 編集日時: 2022 年 8 月 16 日 16:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSTrustedAdvisorPriorityReadOnlyAccess

AWSTrustedAdvisorPriorityReadOnlyAccess は、AWS Trusted Advisor Priority への読み取り専用アクセスを提供する AWS マネージドポリシーです。これには、委任管理者アカウントを閲覧する許可が含まれます。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSTrustedAdvisorPriorityReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 8 月 16 日 16:35 UTC
- 編集日時: 2022 年 8 月 16 日 16:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSTrustedAdvisorReportingServiceRolePolicy

AWSTrustedAdvisorReportingServiceRolePolicy は、Trusted Advisor マルチアカウントレポートのサービスポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 19 日 17:41 UTC
- 編集日時: 2023 年 2 月 28 日 23:23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSTrustedAdvisorServiceRolePolicy

AWSTrustedAdvisorServiceRolePolicy は、コスト削減、パフォーマンス向上、AWS 環境のセキュリティ向上に貢献するために AWS Trusted Advisor サービスへのアクセスに関連する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 2 月 22 日 21:24 UTC
- 編集日時： 2024 年 1 月 18 日 16:25 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v12 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSUserNotificationsServiceLinkedRolePolicy

AWSUserNotificationsServiceLinkedRolePolicy は、ユーザーに代わって AWS ユーザー通知が AWS サービスを呼び出せるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 4 月 19 日 13:28 UTC
- 編集日時: 2023 年 4 月 19 日 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSVendorInsightsAssessorFullAccess

AWSVendorInsightsAssessorFullAccess は、資格のある Vendor Insights リソースの閲覧にフルアクセスを提供し、Vendor Insights サブスクリプションを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSVendorInsightsAssessorFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 7 月 26 日 15:05 UTC
- 編集日時: 2022 年 12 月 1 日 00:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSVendorInsightsAssessorReadOnly

AWSVendorInsightsAssessorReadOnly は、資格のある Vendor Insights リソースを閲覧するための読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSVendorInsightsAssessorReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 7 月 26 日 15:05 UTC
- 編集日時: 2022 年 12 月 1 日 00:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSVendorInsightsVendorFullAccess

AWSVendorInsightsVendorFullAccess は、Vendor Insights リソースの作成および管理するためのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSVendorInsightsVendorFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 7 月 26 日 15:05 UTC
- 編集日時: 2023 年 10 月 19 日 01:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSVendorInsightsVendorReadOnly

AWSVendorInsightsVendorReadOnly は、Vendor Insights リソースを閲覧するための読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSVendorInsightsVendorReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 7 月 26 日 15:05 UTC
- 編集日時: 2022 年 12 月 1 日 00:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSVpcLatticeServiceRolePolicy

AWSVpcLatticeServiceRolePolicy は、VPC Lattice がユーザーに代わって AWS リソースにアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 30 日 20:47 UTC
- 編集日時: 2022 年 11 月 30 日 20:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSVPCS2SVpnServiceRolePolicy

AWSVPCS2SVpnServiceRolePolicy は、Site-to-Site VPN が VPN 接続に関連するリソースを作成および管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 8 月 6 日 14:13 UTC
- 編集日時: 2019 年 8 月 6 日 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSVPCTransitGatewayServiceRolePolicy

AWSVPCTransitGatewayServiceRolePolicy は、VPC Transit Gateway が Transit Gateway VPC アタッチメントに必要なリソースを作成および管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 26 日 16:21 UTC
- 編集日時: 2021 年 4 月 15 日 16:31 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSVPCVerifiedAccessServiceRolePolicy

AWSVPCVerifiedAccessServiceRolePolicy は、AWS Verified Access サービスがユーザーに代わってエンドポイントをプロビジョニングできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 29 日 03:35 UTC
- 編集時間:2023 年 11 月 17 日 21:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSWAFConsoleFullAccess

`AWSWAFConsoleFullAccess` は、AWS Management Console 経由で AWS WAF へのフルアクセスを提供する AWS マネージドポリシーです。このポリシーでは、Amazon CloudFront ディスト

リビューションを一覧表示および更新する許可、AWS Elastic Load Balancing でロードバランサーを表示する許可、Amazon API Gateway の REST API およびステージを表示する許可、Amazon CloudWatch メトリクスを一覧表示して表示する許可、アカウント内で有効になっているリージョンを表示する許可も付与されることにご注意ください。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSWAFConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 4 月 6 日 18:38 UTC
- 編集日時: 2023 年 6 月 5 日 20:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSWAFConsoleReadOnlyAccess

`AWSWAFConsoleReadOnlyAccess` は、AWS Management Console 経由で AWS WAF への読み取り専用アクセスを提供する AWS マネージドポリシーです。このポリシーでは、Amazon CloudFront ディストリビューションを一覧表示する許可、AWS Elastic Load Balancing でロードバランサーを表示する許可、Amazon API Gateway の REST API およびステージを表示する許可、Amazon CloudWatch メトリクスを一覧表示して表示する許可、アカウント内で有効になっているリージョンを表示する許可も付与されることにご注意ください。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSWAFConsoleReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 4 月 6 日 18:43 UTC
- 編集日時: 2023 年 6 月 5 日 20:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSWAFFullAccess

AWSWAFFullAccess は、AWS WAF アクションへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSWAFFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 10 月 6 日 20:44 UTC

- 編集日時: 2023 年 6 月 5 日 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFFullAccess

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSWAFReadOnlyAccess

AWSWAFReadOnlyAccess は、AWS WAF アクションへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSWAFReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 10 月 6 日 20:43 UTC
- 編集日時: 2023 年 6 月 5 日 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSWellArchitectedDiscoveryServiceRolePolicy

`AWSWellArchitectedDiscoveryServiceRolePolicy` は、WellArchitected が顧客に代わって WellArchitected リソースに関連する AWS サービスおよびリソースにアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 4 月 26 日 18:36 UTC
- 編集日時: 2023 年 4 月 26 日 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSWellArchitectedOrganizationsServiceRolePolicy

AWSWellArchitectedOrganizationsServiceRolePolicy は、Well-Architected がユーザーに代わって Organizations にアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 6 月 23 日 17:15 UTC
- 編集日時: 2022 年 7 月 25 日 18:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSWickrFullAccess

AWSWickrFullAccess は、AWS Management Console の Wickr 管理機能を含め、Wickr サービスにすべての管理許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSWickrFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 27 日 20:36 UTC
- 編集日時: 2022 年 11 月 27 日 20:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSWickrFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSXrayCrossAccountSharingConfiguration

AWSXrayCrossAccountSharingConfiguration は、オブザーバビリティ Access Manager のリンクを管理し、X-Ray トレースの共有を確立する機能を提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSXrayCrossAccountSharingConfiguration をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 27 日 13:46 UTC
- 編集日時: 2022 年 11 月 27 日 13:46 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSXRayDaemonWriteAccess

AWSXRayDaemonWriteAccess は、 AWS X-Ray デーモンが生のトレースセグメントデータをサービスの API に中継し、X-Ray SDK で使用するサンプリングデータ (ルール、ターゲットなど) を取得できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSXRayDaemonWriteAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 8 月 28 日 23:00 UTC
- 編集日時 : 2024 年 2 月 13 日 21:58 UTC
- ARN: arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSXrayFullAccess

`AWSXrayFullAccess` は、AWS X-Ray のフルアクセスに関する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSXrayFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 12 月 1 日 18:30 UTC
- 編集日時: 2016 年 12 月 1 日 18:30 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSXrayReadOnlyAccess

`AWSXrayReadOnlyAccess` は、 AWS X-Ray 読み取り専用AWS マネージドポリシーである マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSXrayReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 12 月 1 日 18:27 UTC
- 編集日時： 2024 年 2 月 14 日 00:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

AWSXrayWriteOnlyAccess

AWSXrayWriteOnlyAccess は、AWS X-Ray 書き込み専用に関する AWS マネージドポリシー です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSXrayWriteOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 12 月 1 日 18:19 UTC
- 編集日時: 2018 年 8 月 28 日 23:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

AWSZonalAutoshiftPracticeRunSLRPolicy

AWSZonalAutoshiftPracticeRunSLRPolicyは、AWS ARC ゾーンシフトの練習実行には管理アクセスを提供し、 CloudWatch 練習実行を監視するためのアラームステータスへのアクセスを提供する管理ポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成時間:2023 年 11 月 29 日 17:34 UTC
- 編集時間:2023 年 11 月 29 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

BatchServiceRolePolicy

`BatchServiceRolePolicy` は、AWS Batch サービスが Amazon EC2 や Amazon ECS リソースなど、必要なリソースを管理するためのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 3 月 10 日 06:55 UTC
- 編集時間:2023 年 12 月 5 日 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

Billing

Billing は、請求およびコスト管理の許可を付与する AWS マネージドポリシーです。これには、アカウントの使用状況の閲覧、ならびに予算および支払い方法の修正および閲覧が含まれます。

このポリシーを使用すると

ユーザー、グループおよびロールに Billing をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:33 UTC
- 編集日時： 2024 年 1 月 17 日 18:03 UTC
- ARN: arn:aws:iam::aws:policy/job-function/Billing

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CertificateManagerServiceRolePolicy

`CertificateManagerServiceRolePolicy` は、Amazon Certificate Manager サービスロールに関する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 6 月 25 日 17:56 UTC
- 編集日時: 2020 年 6 月 25 日 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ClientVPNServiceConnectionsRolePolicy

`ClientVPNServiceConnectionsRolePolicy` は、AWS Client VPN が Client VPN エンドポイント接続を管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 8 月 12 日 19:48 UTC
- 編集日時: 2020 年 8 月 12 日 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ClientVPNServiceRolePolicy

`ClientVPNServiceRolePolicy` は、AWS Client VPN が Client VPN エンドポイントを管理できるようにするポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 12 月 10 日 21:20 UTC
- 編集日時: 2020 年 8 月 12 日 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudFormationStackSetsOrgAdminServiceRolePolicy

CloudFormationStackSetsOrgAdminServiceRolePolicy は、CloudFormation StackSets 用 (組織マスターアカウント) サービスロールに関連する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 10 日 00:20 UTC
- 編集日時: 2019 年 12 月 10 日 00:20 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudFormationStackSetsOrgMemberServiceRolePolicy

`CloudFormationStackSetsOrgMemberServiceRolePolicy` は、CloudFormation StackSets (Organization メンバーアカウント) のサービスロールである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 9 日 23:52 UTC
- 編集日時: 2019 年 12 月 9 日 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudFrontFullAccess

`CloudFrontFullAccess` は、 CloudFront コンソールへのフルアクセスと、 経由で Amazon S3 バケットを一覧表示する機能を提供する AWSマネージドポリシーですAWS Management Console。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudFrontFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時： 2024 年 1 月 4 日 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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::*:*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudFrontReadOnlyAccess

`CloudFrontReadOnlyAccess` は、ディス CloudFront トリビューション設定情報へのアクセスを提供し、 経由でディストリビューションを一覧表示する AWSマネージドポリシーですAWS Management Console。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudFrontReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時： 2024 年 1 月 4 日 16:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudHSMServiceRolePolicy

CloudHSMServiceRolePolicy は、CloudHSM が使用または管理する AWS リソースへのアクセスを可能にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 6 日 19:12 UTC
- 編集日時: 2017 年 11 月 6 日 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudSearchFullAccess

CloudSearchFullAccess は、Amazon CloudSearch 設定サービスへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudSearchFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2015 年 2 月 6 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/CloudSearchFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudSearchReadOnlyAccess

`CloudSearchReadOnlyAccess` は、Amazon CloudSearch 設定サービスへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudSearchReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2015 年 2 月 6 日 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:Describe*",
        "cloudsearch:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudTrailServiceRolePolicy

`CloudTrailServiceRolePolicy`は、AWS次のような管理ポリシーです。 CloudTrail ServiceLinkedRole

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 10 月 24 日 21:21 UTC
- 編集時間:2023 年 11 月 27 日 01:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatch-CrossAccountAccess

`CloudWatch-CrossAccountAccess` は、CloudWatch が現在のアカウントに代わってリモートアカウントの CloudWatch-CrossAccountSharing ロールを引き受け、データクロスアカウントおよびクロスリージョンを表示できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 7 月 23 日 09:59 UTC
- 編集日時: 2019 年 7 月 23 日 09:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchActionsEC2Access

CloudWatchActionsEC2Access は、CloudWatch アラームおよびメトリクスの他に、EC2 メタデータに読み取り専用のアクセスを提供する AWS マネージドポリシーです。EC2 インスタンスを停止、終了、再起動するためのアクセスを提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchActionsEC2Access をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 7 月 7 日 00:00 UTC
- 編集日時: 2015 年 7 月 7 日 00:00 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchActionsEC2Access

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchAgentAdminPolicy

`CloudWatchAgentAdminPolicy` は、 を使用するために必要な完全なアクセス許可を持つ AWSマネージドポリシーです AmazonCloudWatchAgent。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchAgentAdminPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 3 月 7 日 00:52 UTC

- 編集日時： 2024 年 2 月 5 日 20:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchAgentServerPolicy

CloudWatchAgentServerPolicy は、 サーバー AmazonCloudWatchAgent で を使用するために必要なアクセス許可に関する AWSマネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchAgentServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 3 月 7 日 01:06 UTC
- 編集日時： 2024 年 2 月 6 日 16:37 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchApplicationInsightsFullAccess

CloudWatchApplicationInsightsFullAccess は、CloudWatch Application Insights および必要な依存関係へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchApplicationInsightsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 11 月 24 日 18:44 UTC
- 編集日時: 2022 年 1 月 25 日 17:51 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
```

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchApplicationInsightsReadOnlyAccess

`CloudWatchApplicationInsightsReadOnlyAccess` は、CloudWatch Application Insights への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchApplicationInsightsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 11 月 24 日 18:48 UTC
- 編集日時: 2020 年 11 月 24 日 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudwatchApplicationInsightsServiceLinkedRolePolicy

`CloudwatchApplicationInsightsServiceLinkedRolePolicy` は、CloudWatch Application Insights のサービスリンクロールポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 12 月 1 日 16:22 UTC

- 編集日時: 2023 年 5 月 11 日 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v24 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchApplicationSignalsServiceRolePolicy

CloudWatchApplicationSignalsServiceRolePolicy は、Application Signals CloudWatch に他の関連 AWS サービスからモニタリングおよびタグ付けデータを収集するアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 9 日 18:09 UTC
- 編集日時： 2024 年 3 月 7 日 00:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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}"
        }
      }
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

CloudWatchAutomaticDashboardsAccess

`CloudWatchAutomaticDashboardsAccess` は、Lambda 関数などのオブジェクトのコンテンツなど、CloudWatch 自動ダッシュボードの表示に使用される CloudWatch 以外の API へのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchAutomaticDashboardsAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 7 月 23 日 10:01 UTC
- 編集日時: 2021 年 4 月 20 日 13:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchCrossAccountSharingConfiguration

CloudWatchCrossAccountSharingConfiguration は、オブザーバビリティ Access Manager のリンクを管理し、CloudWatch リソースの共有を確立する機能を提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchCrossAccountSharingConfiguration をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 27 日 14:01 UTC
- 編集日時: 2022 年 11 月 27 日 14:01 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchEventsBuiltInTargetExecutionAccess

`CloudWatchEventsBuiltInTargetExecutionAccess` は、Amazon CloudWatch Events の組み込みターゲットがユーザーに代わって EC2 アクションを実行できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchEventsBuiltInTargetExecutionAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 1 月 14 日 18:35 UTC
- 編集日時: 2016 年 1 月 14 日 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchEventsFullAccess

`CloudWatchEventsFullAccess` は、Amazon CloudWatch Events へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchEventsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 1 月 14 日 18:37 UTC
- 編集日時: 2022 年 12 月 1 日 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchEventsInvocationAccess

CloudWatchEventsInvocationAccess は、Amazon CloudWatch Events がユーザーアカウントの AWS Kinesis Stream 内のストリームにイベントを中継できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchEventsInvocationAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 1 月 14 日 18:36 UTC
- 編集日時: 2016 年 1 月 14 日 18:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchEventsReadOnlyAccess

`CloudWatchEventsReadOnlyAccess` は、Amazon CloudWatch Events への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchEventsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 1 月 14 日 18:27 UTC
- 編集日時: 2022 年 12 月 1 日 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchEventsServiceRolePolicy

`CloudWatchEventsServiceRolePolicy` は、AWS CloudWatch がユーザーに代わってアラームおよびイベントで設定されたアクションを実行できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 17 日 00:42 UTC
- 編集日時: 2017 年 11 月 17 日 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchFullAccess

`CloudWatchFullAccess` は、CloudWatch へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2022 年 11 月 27 日 13:23 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchFullAccessV2

`CloudWatchFullAccessV2`AWSは次のような管理ポリシーです CloudWatch。へのフルアクセスを提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchFullAccessV2` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 8 月 1 日 11:32 UTC
- 編集時間:2023 年 12 月 5 日 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccessV2`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchInternetMonitorServiceRolePolicy

`CloudWatchInternetMonitorServiceRolePolicy` は、Internet Monitor がユーザーに代わって EC2、Workspaces、CloudFront リソース、その他の必要なサービスにアクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 27 日 17:46 UTC
- 編集日時: 2023 年 7 月 20 日 04:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchLambdaInsightsExecutionRolePolicy

CloudWatchLambdaInsightsExecutionRolePolicy は、Lambda Insights 拡張機能に必要な AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchLambdaInsightsExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 10 月 7 日 19:27 UTC
- 編集日時: 2020 年 10 月 7 日 19:27 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchLogsCrossAccountSharingConfiguration

CloudWatchLogsCrossAccountSharingConfiguration は、オブザーバビリティ Access Manager のリンクを管理し、CloudWatch のログリソースの共有を確立する機能を提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchLogsCrossAccountSharingConfiguration をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 27 日 13:55 UTC
- 編集日時: 2022 年 11 月 27 日 13:55 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchLogsFullAccess

`CloudWatchLogsFullAccess`AWS CloudWatch ログへのフルアクセスを提供する管理ポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchLogsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集時間:2023 年 11 月 26 日 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchLogsReadOnlyAccess

`CloudWatchLogsReadOnlyAccess`AWSは次のような管理ポリシーです。 CloudWatch ログへの読み取り専用アクセスを提供します

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchLogsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集時間:2023 年 11 月 26 日 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchNetworkMonitorServiceRolePolicy

CloudWatchNetworkMonitorServiceRolePolicyは、AWSユーザーに代わって CloudWatch Network Monitor が EC2 と VPC リソースにアクセスして管理し、データを公開したり、CloudWatch 他の必要なサービスにアクセスしたりすることを許可する管理ポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成時間:2023 年 12 月 21 日 18:53 UTC
- 編集時間:2023 年 12 月 21 日 18:53 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchReadOnlyAccess

`CloudWatchReadOnlyAccess`AWSは次のような管理ポリシーです CloudWatch。への読み取り専用アクセスを提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集時間:2023 年 12 月 5 日 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchSyntheticsFullAccess

`CloudWatchSyntheticsFullAccess` は、CloudWatch Synthetics へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchSyntheticsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 11 月 25 日 17:39 UTC
- 編集日時: 2022 年 5 月 6 日 18:14 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CloudWatchSyntheticsReadOnlyAccess

`CloudWatchSyntheticsReadOnlyAccess` は、CloudWatch Synthetics への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchSyntheticsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 11 月 25 日 17:45 UTC
- 編集日時: 2020 年 3 月 6 日 19:26 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ComprehendDataAccessRolePolicy

`ComprehendDataAccessRolePolicy` は、データアクセスのための S3 リソースへのアクセスをできるようにする AWS Comprehend サービスロール用の AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ComprehendDataAccessRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 3 月 6 日 22:28 UTC
- 編集日時: 2019 年 3 月 6 日 22:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*Comprehend*",
      "arn:aws:s3:::*comprehend*"
    ]
  }
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ComprehendFullAccess

`ComprehendFullAccess` は、Amazon Comprehend へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ComprehendFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 29 日 18:08 UTC
- 編集日時: 2017 年 12 月 5 日 01:36 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ComprehendMedicalFullAccess

`ComprehendMedicalFullAccess` は、Amazon Comprehend Medical へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ComprehendMedicalFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 27 日 17:55 UTC
- 編集日時: 2018 年 11 月 27 日 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ComprehendReadOnly

`ComprehendReadOnly` は、Amazon Comprehend への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ComprehendReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 29 日 18:10 UTC
- 編集日時: 2022 年 4 月 26 日 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ComputeOptimizerReadOnlyAccess

`ComputeOptimizerReadOnlyAccess` は、ComputeOptimizer への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ComputeOptimizerReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 3 月 7 日 00:11 UTC
- 編集日時: 2023 年 8 月 28 日 19:22 UTC
- ARN: arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ComputeOptimizerServiceRolePolicy

`ComputeOptimizerServiceRolePolicy` は、ComputeOptimizer がユーザーに代わって AWS サービスを呼び出してワークロードの詳細を収集できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2019 年 12 月 3 日 08:45 UTC
- 編集日時: 2022 年 6 月 13 日 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ConfigConformsServiceRolePolicy

`ConfigConformsServiceRolePolicy` は、AWSConfig がコンフォーマンスパックを作成するために必要な AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 7 月 25 日 21:38 UTC
- 編集日時: 2023 年 1 月 12 日 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CostOptimizationHubAdminAccess

CostOptimizationHubAdminAccessAWSは次のような管理ポリシーです。この管理ポリシーは、Cost Optimization Hub への管理者アクセスを提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに CostOptimizationHubAdminAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時間:2023 年 12 月 19 日 00:03 UTC
- 編集時間:2023 年 12 月 19 日 00:03 UTC
- ARN: arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CostOptimizationHubReadOnlyAccess

`CostOptimizationHubReadOnlyAccess`AWSは次のような管理ポリシーです。この管理ポリシーは Cost Optimization Hub への読み取り専用アクセスを提供します。

このポリシーを使用すると

ユーザー、グループおよびロールに `CostOptimizationHubReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時間:2023 年 12 月 13 日 18:04 UTC
- 編集時間:2023 年 12 月 13 日 18:04 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CostOptimizationHubServiceRolePolicy

CostOptimizationHubServiceRolePolicyは、Cost Optimization Hub が組織情報を取得し、AWS最適化関連のデータとメタデータを収集できるようにする管理ポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成時間:2023 年 11 月 26 日 08:03 UTC
- 編集時間:2023 年 11 月 26 日 08:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

CustomerProfilesServiceLinkedRolePolicy

`CustomerProfilesServiceLinkedRolePolicy` は、Amazon Connect Customer Profiles がユーザーに代わって AWS サービスおよびリソースにアクセスできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2023 年 3 月 7 日 22:56 UTC
- 編集日時: 2023 年 3 月 7 日 22:56 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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_*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

DatabaseAdministrator

DatabaseAdministrator は、AWS データベースサービスの設定と構成に必要な AWS サービスおよびアクションをアクセスする許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに DatabaseAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:25 UTC
- 編集日時: 2019 年 1 月 8 日 00:48 UTC
- ARN: arn:aws:iam::aws:policy/job-function/DatabaseAdministrator

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
```

```
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

DataScientist

`DataScientist` は、AWS データ分析サービスに許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `DataScientist` をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:28 UTC
- 編集日時: 2019 年 12 月 3 日 16:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DataScientist`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

DAXServiceRolePolicy

DAXServiceRolePolicy は、DAX が顧客に代わってネットワークインターフェイス、セキュリティグループ、サブネット、VPC を作成および管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 3 月 5 日 17:51 UTC
- 編集日時: 2018 年 3 月 5 日 17:51 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

DynamoDBCloudWatchContributorInsightsServiceRolePolicy は、Amazon DynamoDB の Amazon CloudWatch Contributor Insights をサポートするために必要な許可に関する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 15 日 21:13 UTC
- 編集日時: 2019 年 11 月 15 日 21:13 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

DynamoDBKinesisReplicationServiceRolePolicy

DynamoDBKinesisReplicationServiceRolePolicy は、AWS DynamoDB に KinesisDataStreams へのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 12 日 00:43 UTC
- 編集日時: 2020 年 11 月 12 日 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

DynamoDBReplicationServiceRolePolicy

DynamoDBReplicationServiceRolePolicy は、DynamoDB がクロスリージョンデータのレプリケーションを行うために必要な許可に関する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 9 日 23:55 UTC
- 編集日時： 2024 年 1 月 8 日 20:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

EC2FastLaunchServiceRolePolicy

EC2FastLaunchServiceRolePolicy は、ec2fastlaunch が顧客のアカウントでプロビジョニングされたスナップショットの作成および管理、および関連メトリクスの公開を許可する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 1 月 10 日 13:08 UTC
- 編集日時: 2022 年 1 月 10 日 13:08 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

EC2FleetTimeShiftableServiceRolePolicy

EC2FleetTimeShiftableServiceRolePolicy は、EC2 フリートが今後インスタンスを起動する許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 23 日 19:47 UTC
- 編集日時: 2019 年 12 月 23 日 19:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

Ec2ImageBuilderCrossAccountDistributionAccess

`Ec2ImageBuilderCrossAccountDistributionAccess` は、EC2 Image Builder がアカウント間のディストリビューションを実行するために必要な許可に関する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `Ec2ImageBuilderCrossAccountDistributionAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 9 月 30 日 19:22 UTC
- 編集日時: 2020 年 9 月 30 日 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

EC2ImageBuilderLifecycleExecutionPolicy

`EC2ImageBuilderLifecycleExecutionPolicy`AWSは次のような管理ポリシーです。EC2 ImageBuilderLifecycleExecutionPolicy ポリシーは、イメージライフサイクル管理タスクの自動ルールをサポートするために、Image Builder のイメージリソースとその基盤となるリソース (AMI、スナップショット) の廃止または削除などのアクションを実行する権限を Image Builder に付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに EC2ImageBuilderLifecycleExecutionPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成時間:2023 年 11 月 16 日 23:23 (UTC)
- 編集時間:2023 年 11 月 16 日 23:23 UTC
- ARN: arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

EC2InstanceConnect

`EC2InstanceConnect` は、お客様が EC2 Instance Connect を呼び出して EC2 インスタンスにエフェメラルキーを公開し、ssh または EC2 Instance Connect CLI 経由で接続できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `EC2InstanceConnect` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2019 年 6 月 27 日 18:53 UTC
- 編集日時: 2019 年 6 月 27 日 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

Ec2InstanceConnectEndpoint

`Ec2InstanceConnectEndpoint` は、顧客が作成した EC2 インスタンス Connect エンドポイントを管理する EC2 インスタンス Connect エンドポイントポリシーに関連する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 1 月 24 日 20:19 UTC
- 編集日時: 2023 年 1 月 24 日 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

EC2InstanceProfileForImageBuilder

`EC2InstanceProfileForImageBuilder` は、Image Builder サービスの EC2 インスタンスプロファイルに関する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに EC2InstanceProfileForImageBuilder をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 1 日 19:08 UTC
- 編集日時: 2020 年 8 月 27 日 16:40 UTC
- ARN: arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

EC2InstanceProfileForImageBuilderECRContainerBuilds

`EC2InstanceProfileForImageBuilderECRContainerBuilds` は、EC2 Image Builder を使用してコンテナイメージを構築するための EC2 インスタンスプロファイルに関する AWS マネージドポリシーです。このポリシーは、ユーザーが ECR イメージをアップロードするために広範な許可を付与します。

このポリシーを使用すると

ユーザー、グループおよびロールに EC2InstanceProfileForImageBuilderECRContainerBuilds をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 12 月 11 日 19:48 UTC
- 編集日時: 2020 年 12 月 11 日 19:48 UTC
- ARN: arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ECRReplicationServiceRolePolicy

ECRReplicationServiceRolePolicy は、ECR Replication が使用または管理する AWS のサービス およびリソースへのアクセスをできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 4 日 22:11 UTC
- 編集日時: 2020 年 12 月 4 日 22:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
```

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ElastiCacheServiceRolePolicy

ElastiCacheServiceRolePolicyAWSは次のような管理ポリシーです。このポリシーでは ElastiCache 、AWSキャッシュの管理に必要なリソースをユーザーに代わって管理できます。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 12 月 7 日 17:50 UTC
- 編集時間:2023 年 11 月 28 日 03:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ElasticLoadBalancingFullAccess

`ElasticLoadBalancingFullAccess` は、Amazon ElasticLoadBalancing へのフルアクセスを提供し、ElasticLoadBalancing 機能の提供に必要な他のサービスへの制限付きアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ElasticLoadBalancingFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 9 月 20 日 20:42 UTC
- 編集日時: 2022 年 11 月 29 日 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
```

```
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ElasticLoadBalancingReadOnly

`ElasticLoadBalancingReadOnly`AWSは次のような管理ポリシーです。Amazon ElasticLoadBalancing および依存サービスへの読み取り専用アクセスを提供します

このポリシーを使用すると

ユーザー、グループおよびロールに `ElasticLoadBalancingReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 9 月 20 日 20:17 UTC
- 編集時間:2023 年 11 月 26 日 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する

- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ElementalActivationsDownloadSoftwareAccess

ElementalActivationsDownloadSoftwareAccess は、購入したアセットを表示したり、関連ソフトウェアやキックスタートファイルをダウンロードしたりするためのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ElementalActivationsDownloadSoftwareAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 9 月 8 日 17:26 UTC
- 編集日時: 2020 年 9 月 8 日 17:26 UTC
- ARN: arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:Download*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ElementalActivationsFullAccess

`ElementalActivationsFullAccess` は、Elemental Appliance および Software で購入した資産を閲覧するためのフルアクセスおよびアクションの実行に関する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ElementalActivationsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 6 月 4 日 21:00 UTC
- 編集日時: 2020 年 6 月 4 日 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ElementalActivationsGenerateLicenses

`ElementalActivationsGenerateLicenses` は、購入済み資産を閲覧するためにアクセスしたり、保留中のアクティベーションのソフトウェアライセンスを生成したりすることに関する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ElementalActivationsGenerateLicenses` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 8 月 28 日 18:28 UTC
- 編集日時: 2020 年 8 月 28 日 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ElementalActivationsReadOnlyAccess

ElementalActivationsReadOnlyAccess は、ユーザーの AWS アカウント に関連する購入済みアセットの詳細リストへの読み取り専用アクセス権限に関する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ElementalActivationsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 8 月 28 日 16:51 UTC
- 編集日時: 2020 年 8 月 28 日 16:51 UTC
- ARN: arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*"
      ],
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ElementalAppliancesSoftwareFullAccess

`ElementalAppliancesSoftwareFullAccess` は、Elemental アプライアンスとソフトウェアの見積もりおよび注文の閲覧および処理のフルアクセスに関する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ElementalAppliancesSoftwareFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 7 月 31 日 16:28 UTC
- 編集日時: 2021 年 2 月 5 日 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ElementalAppliancesSoftwareReadOnlyAccess

`ElementalAppliancesSoftwareReadOnlyAccess` は、Elemental アプライアンスとソフトウェアの見積もりおよび注文を閲覧する読み取り専用アクセスに関する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ElementalAppliancesSoftwareReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 4 月 1 日 22:31 UTC
- 編集日時: 2020 年 4 月 1 日 22:31 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ElementalSupportCenterFullAccess

`ElementalSupportCenterFullAccess` は、Elemental アプライアンスとソフトウェアのサポートケースおよび製品サポートコンテンツの閲覧および処理を行うためのフルアクセスに関する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ElementalSupportCenterFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 11 月 25 日 18:08 UTC
- 編集日時: 2021 年 2 月 5 日 21:02 UTC
- ARN: arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

EMRDescribeClusterPolicyForEMRWAL

EMRDescribeClusterPolicyForEMRWAL は、Amazon EMR の WAL サービスがクラスターのステータスを検索して返せるようにする読み取り専用許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 6 月 15 日 23:30 UTC
- 編集日時: 2023 年 6 月 15 日 23:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

FMSServiceRolePolicy

FMSServiceRolePolicy は、FM Service Linked Role が顧客の AWS Organization アカウント内の FM 管理リソースで FM 関連アクションを実行できるようにするアクセスポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 3 月 28 日 23:01 UTC
- 編集日時: 2023 年 4 月 21 日 18:33 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v28 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

FSxDeleteServiceLinkedRoleAccess

FSxDeleteServiceLinkedRoleAccess は、Amazon FSx が Amazon S3 にアクセスするための Service Linked Roles を削除することを許可する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 28 日 10:40 UTC
- 編集日時: 2018 年 11 月 28 日 10:40 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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_*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

GameLiftGameServerGroupPolicy

`GameLiftGameServerGroupPolicy` は、Gamelift GameServerGroups が顧客リソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `GameLiftGameServerGroupPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2020 年 4 月 3 日 23:12 UTC
- 編集日時: 2020 年 5 月 13 日 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

GlobalAcceleratorFullAccess

GlobalAcceleratorFullAccess は、GlobalAccelerator ユーザーがすべての API へのフルアクセスをできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに GlobalAcceleratorFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 27 日 02:44 UTC
- 編集日時: 2020 年 12 月 4 日 19:17 UTC
- ARN: arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

GlobalAcceleratorReadOnlyAccess

`GlobalAcceleratorReadOnlyAccess` は、GlobalAccelerator ユーザーが読み取り専用 API へのアクセスをできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `GlobalAcceleratorReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 27 日 02:41 UTC
- 編集日時: 2018 年 11 月 27 日 02:41 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

GreengrassOTAUpdateArtifactAccess

`GreengrassOTAUpdateArtifactAccess` は、すべての Greengrass リージョンにある Greengrass OTA アップデートアーティファクトへの読み取りアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `GreengrassOTAUpdateArtifactAccess` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 11 月 29 日 18:11 UTC
- 編集日時: 2018 年 12 月 18 日 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
      ]
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

GroundTruthSyntheticConsoleFullAccess

GroundTruthSyntheticConsoleFullAccess は、SageMaker Ground Truth 合成コンソールのすべての機能を使用するために必要な許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに GroundTruthSyntheticConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2022 年 8 月 25 日 15:58 UTC
- 編集日時: 2022 年 8 月 25 日 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

GroundTruthSyntheticConsoleReadOnlyAccess

`GroundTruthSyntheticConsoleReadOnlyAccess` は、AWS Management Console 経由で SageMaker Ground Truth Synthetic への読み取り専用アクセスを付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `GroundTruthSyntheticConsoleReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 8 月 25 日 15:58 UTC
- 編集日時: 2022 年 8 月 25 日 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

Health_OrganizationsServiceRolePolicy

`Health_OrganizationsServiceRolePolicy` は、組織ビュー機能を有効にする AWS Health に関する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 16 日 13:28 UTC
- 編集日時： 2024 年 2 月 6 日 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

IAMAccessAdvisorReadOnly

IAMAccessAdvisorReadOnly は、サービスの最終アクセス情報など、IAM アクセスアドバイザーが提供するすべてのアクセス情報を読み取るためのアクセスを付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに IAMAccessAdvisorReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 6 月 21 日 19:33 UTC

- 編集日時: 2019 年 6 月 21 日 19:33 UTC
- ARN: arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

IAMAccessAnalyzerFullAccess

`IAMAccessAnalyzerFullAccess` は、IAM Access Analyzer へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `IAMAccessAnalyzerFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 2 日 17:12 UTC
- 編集日時: 2019 年 12 月 2 日 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

IAMAccessAnalyzerReadOnlyAccess

`IAMAccessAnalyzerReadOnlyAccess` は、IAM Access Analyzer リソースへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `IAMAccessAnalyzerReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 12 月 2 日 17:12 UTC
- 編集時間:2023 年 11 月 27 日 02:24 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

IAMFullAccess

`IAMFullAccess` は、AWS Management Console 経由で IAM へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `IAMFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2019 年 6 月 21 日 19:40 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する

- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

IAMReadOnlyAccess

IAMReadOnlyAccess は、AWS Management Console 経由で IAM への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに IAMReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2018 年 1 月 25 日 19:11 UTC
- ARN: arn:aws:iam::aws:policy/IAMReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
```

```
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

IAMSelfManageServiceSpecificCredentials

IAMSelfManageServiceSpecificCredentials は、IAM ユーザーが自身のサービス固有の認証情報を管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに IAMSelfManageServiceSpecificCredentials をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 12 月 22 日 17:25 UTC
- 編集日時: 2016 年 12 月 22 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

IAMUserChangePassword

`IAMUserChangePassword` は、IAM ユーザーが自身のパスワードを変更できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `IAMUserChangePassword` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 11 月 15 日 00:25 UTC
- 編集日時: 2016 年 11 月 15 日 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserChangePassword`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

IAMUserSSHKeys

`IAMUserSSHKeys` は、IAM ユーザーが自身の SSH キーを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `IAMUserSSHKeys` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 7 月 9 日 17:08 UTC
- 編集日時: 2015 年 7 月 9 日 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserSSHKeys`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

IVSFullAccess

`IVSFullAccess`は、Interactive Video Service（IVS）へのフルアクセスを提供し、AWSivsコンソールへのフルアクセスに必要な依存サービスの権限も提供する管理ポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `IVSFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時間:2023 年 12 月 13 日 21:20 UTC
- 編集時間:2023 年 12 月 13 日 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/IVSFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

IVSReadOnlyAccess

`IVSReadOnlyAccess` は、IVS 低レイテンシーおよびリアルタイムストリーミング APIs への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに IVSReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時刻: 2023 年 12 月 5 日 18:00 UTC
- 編集日時： 2024 年 2 月 16 日 18:03 UTC
- ARN: arn:aws:iam::aws:policy/IVSReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

IVSRecordToS3

IVSRecordToS3 は、IVS ライブストリームの録画に S3 PutObject を実行する Service Linked Role に関する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 5 日 00:10 UTC
- 編集日時: 2020 年 12 月 5 日 00:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

KafkaConnectServiceRolePolicy

KafkaConnectServiceRolePolicy は、Kafka Connect がユーザーに代わって AWS リソースを管理する許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 9 月 7 日 13:12 UTC
- 編集日時: 2021 年 9 月 7 日 13:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
```

```
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

KafkaServiceRolePolicy

KafkaServiceRolePolicy は、 Kafka の IAM サービスリンクロールポリシー に関する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 15 日 23:31 UTC
- 編集日時: 2023 年 4 月 28 日 00:39 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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_*"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

KeyspacesReplicationServiceRolePolicy

KeyspacesReplicationServiceRolePolicy は、クロスリージョンデータレプリケーションに Keyspaces が要求する許可に関する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 5 月 2 日 16:15 UTC
- 編集日時: 2023 年 5 月 2 日 16:15 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:SelectMultiRegionResource",
        "cassandra:Modify",
        "cassandra:ModifyMultiRegionResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

LakeFormationDataAccessServiceRolePolicy

`LakeFormationDataAccessServiceRolePolicy` は、Lake Formation リソースへの一時的なデータアクセスの付与に関する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 20 日 20:46 UTC
- 編集日時： 2024 年 2 月 6 日 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

LexBotPolicy

LexBotPolicy は、AWS Lex Bot ユースケースに関する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 2 月 17 日 22:18 UTC
- 編集日時: 2019 年 11 月 13 日 22:29 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectSentiment"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

LexChannelPolicy

LexChannelPolicy は、AWS Lex Channel ユースケースに関する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 2 月 17 日 23:23 UTC
- 編集日時: 2017 年 2 月 17 日 23:23 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

LightsailExportAccess

`LightsailExportAccess` は、リソースをエクスポートする許可を付与する AWS Lightsail Service Linked Role Policy に関する AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 9 月 28 日 16:35 UTC
- 編集日時: 2022 年 1 月 15 日 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

MediaConnectGatewayInstanceRolePolicy

`MediaConnectGatewayInstanceRolePolicy` は、MediaConnect Gateway インスタンスを MediaConnect Gateway に登録する許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `MediaConnectGatewayInstanceRolePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 3 月 22 日 20:43 UTC
- 編集日時: 2023 年 3 月 22 日 20:43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:PollGateway",
        "mediaconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

MediaPackageServiceRolePolicy

`MediaPackageServiceRolePolicy` は、MediaPackage が CloudWatch にログを公開できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 9 月 18 日 17:45 UTC
- 編集日時: 2020 年 9 月 18 日 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

MemoryDBServiceRolePolicy

MemoryDBServiceRolePolicy は、MemoryDB がユーザーに代わり、必要に応じて AWS リソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 8 月 17 日 22:34 UTC
- 編集日時: 2021 年 8 月 18 日 23:48 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

MigrationHubDMSAccessServiceRolePolicy

MigrationHubDMSAccessServiceRolePolicy は Database Migration Service のポリシーであり、顧客のアカウントのロールを引き受けて Migration Hub を呼び出す AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 12 日 17:50 UTC
- 編集日時: 2019 年 10 月 7 日 17:57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

MigrationHubServiceRolePolicy

`MigrationHubServiceRolePolicy` は、Migration Hub がユーザーに代わって Application Discovery Service 呼び出せるようにする AWS マネージドポリシー です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 12 日 17:22 UTC
- 編集日時: 2020 年 8 月 6 日 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

MigrationHubSMSAccessServiceRolePolicy

MigrationHubSMSAccessServiceRolePolicy は、Server Migration Service のポリシーであり、顧客アカウントのロールを引き受けて Migration Hub を呼び出す AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 12 日 18:30 UTC
- 編集日時: 2019 年 10 月 7 日 18:02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

MonitronServiceRolePolicy

MonitronServiceRolePolicy は、 AWS Monitron サービスリンクロール用の、必要な顧客リソースにアクセスを付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 5 月 2 日 19:22 UTC
- 編集日時: 2022 年 5 月 2 日 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

NeptuneConsoleFullAccess

NeptuneConsoleFullAccess は、AWS Management Consoleを使用して Amazon Neptune を管理するためのフルアクセスを提供する AWS マネージドポリシーです。このポリシーでは、アカウント内のすべての SNS トピックを公開するためのフルアクセス、Amazon EC2 インスタンスおよび VPC 設定を作成および編集する許可、Amazon KMS でキーを表示および一覧表示する許可、Amazon RDS へのフルアクセスも付与されることにご注意ください。詳細については、https://aws.amazon.com/neptune/faqs/ を参照してください。

このポリシーを使用すると

ユーザー、グループおよびロールに NeptuneConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 6 月 19 日 21:35 UTC
- 編集時間:2023 年 11 月 30 日 07:32 UTC
- ARN: arn:aws:iam::aws:policy/NeptuneConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

NeptuneFullAccess

NeptuneFullAccess は、Amazon Neptune へのフルアクセスを提供する AWS マネージドポリシーです。このポリシーでは、アカウント内のすべての SNS トピックに公開するためのフルアクセスおよび Amazon RDS へのフルアクセスも付与されることにご注意ください。詳細については、https://aws.amazon.com/neptune/faqs/ を参照してください。

このポリシーを使用すると

ユーザー、グループおよびロールに NeptuneFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 5 月 30 日 19:17 UTC

- 編集日時： 2024 年 1 月 22 日 16:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
```

```
      ]
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

NeptuneGraphReadOnlyAccess

`NeptuneGraphReadOnlyAccess`は、Amazon Neptune Analytics のすべてのリソースへの読み取り専用アクセスと、AWS依存サービスの読み取り専用アクセス権限を提供する管理ポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `NeptuneGraphReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成時間:2023 年 11 月 30 日 07:32 UTC
- 編集時間:2023 年 11 月 30 日 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
      ]
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

NeptuneReadOnlyAccess

NeptuneReadOnlyAccess は、Amazon Neptune への読み取り専用アクセスを提供する AWS マネージドポリシーです。このポリシーでは、Amazon RDS リソースへのアクセスも付与されることにご注意ください。詳細については、https://aws.amazon.com/neptune/faqs/ を参照してください。

このポリシーを使用すると

ユーザー、グループおよびロールに NeptuneReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー

- 作成日時: 2018 年 5 月 30 日 19:16 UTC
- 編集日時： 2024 年 1 月 22 日 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

NetworkAdministrator

NetworkAdministrator は、AWS ネットワークリソースの設定および構成に必要な AWS サービスおよびアクションへのフルアクセス許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに NetworkAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:31 UTC
- 編集日時: 2021 年 9 月 16 日 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/NetworkAdministrator`

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント


```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

OAMFullAccess

OAMFullAccess は、CloudWatch オブザーバビリティ Access Manager へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに OAMFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 27 日 13:38 UTC
- 編集日時: 2022 年 11 月 27 日 13:38 UTC
- ARN: arn:aws:iam::aws:policy/OAMFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

OAMReadOnlyAccess

`OAMReadOnlyAccess` は、CloudWatch Observability Access Manager への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `OAMReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 11 月 27 日 13:29 UTC
- 編集日時: 2022 年 11 月 27 日 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/OAMReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

PartnerCentralAccountManagementUserRoleAssociation

`PartnerCentralAccountManagementUserRoleAssociation` は、パートナーセントラルのユーザーを IAM ロールに関連付けおよび関連付け解除するためのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `PartnerCentralAccountManagementUserRoleAssociation` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 11 月 10 日 02:03 UTC

- 編集日時: 2023 年 11 月 10 日 02:03 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
```

```
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

PowerUserAccess

PowerUserAccess は、AWS サービスおよびリソースへのフルアクセスを提供しますが、ユーザーおよびグループの管理を許可しない AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに PowerUserAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2023 年 7 月 6 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/PowerUserAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

`QuickSightAccessForS3StorageManagementAnalyticsReadOnly` は、QuickSight チームが S3 ストレージ管理分析によって作成された顧客データにアクセスするために使用する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに QuickSightAccessForS3StorageManagementAnalyticsReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 6 月 12 日 18:18 UTC
- 編集日時: 2019 年 10 月 8 日 23:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

RDSCloudHsmAuthorizationRole

RDSCloudHsmAuthorizationRole は、Amazon RDS サービスロールのデフォルトの AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに RDSCloudHsmAuthorizationRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2019 年 9 月 26 日 22:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm:DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ReadOnlyAccess

`ReadOnlyAccess` は、 AWS サービスとリソースへの読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時： 2024 年 2 月 5 日 15:00 UTC
- ARN: `arn:aws:iam::aws:policy/ReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v111 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

ResourceGroupsandTagEditorFullAccess

`ResourceGroupsandTagEditorFullAccess` は、Resource Groups およびタグエディタへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ResourceGroupsandTagEditorFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2023 年 8 月 10 日 13:29 UTC
- ARN: arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
```

```
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ResourceGroupsandTagEditorReadOnlyAccess

`ResourceGroupsandTagEditorReadOnlyAccess` は、Resource Groups およびタグエディターを使用するためのアクセスを提供しますが、タグエディター経由でタグの編集は許可しない AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ResourceGroupsandTagEditorReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2023 年 8 月 10 日 13:42 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ResourceGroupsServiceRolePolicy

`ResourceGroupsServiceRolePolicy` は、AWS Resource Groups がリソースを所有する AWS サービスにクエリを実行し、グループを最新の状態に維持できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 1 月 5 日 16:57 UTC
- 編集日時: 2023 年 1 月 5 日 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ROSAAmazonEBSCSIDriverOperatorPolicy

ROSAAmazonEBSCSIDriverOperatorPolicy は、OpenShift Amazon EBS Container Storage Interface (CSI) ドライバーオペレーターが Red Hat OpenShift Service on AWS (ROSA) クラスターに Amazon EBS CSI ドライバーをインストールして管理できるようにする AWS マネージドポリシーです。Amazon EBS CSI ドライバーは、ROSA クラスターが永続ボリューム用 Amazon EBS ボリュームのライフサイクルを管理できるようにします。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAAmazonEBSCSIDriverOperatorPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 20 日 22:36 UTC
- 編集日時: 2023 年 4 月 20 日 22:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ROSACloudNetworkConfigOperatorPolicy

ROSACloudNetworkConfigOperatorPolicy は、OpenShift クラウドネットワーク Config コントローラーオペレーターが AWS (ROSA) クラスターネットワークオーバーレイ上の Red Hat OpenShift Service が使用するネットワークリソースをプロビジョニングおよび管理できるようにする AWS マネージドポリシーです。OpenShift クラウドネットワークオペレーターは、CustomResourceDefinitions 経由でネットワークプラグインに代わって AWS API と対話します。オペレーターはこれらのポリシー許可を使用し、ROSA クラスターの一部として Amazon EC2 インスタンスのプライベート IP アドレスを管理します。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSACloudNetworkConfigOperatorPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 20 日 22:34 UTC
- 編集日時: 2023 年 4 月 20 日 22:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ROSAControlPlaneOperatorPolicy

ROSAControlPlaneOperatorPolicy は、AWS (ROSA) コントロールプレーン上の Red Hat OpenShift Service が ROSA クラスターの Amazon EC2 および Amazon Route 53 リソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAControlPlaneOperatorPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 24 日 23:02 UTC
- 編集日時: 2023 年 6 月 30 日 21:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ROSAImageRegistryOperatorPolicy

ROSAImageRegistryOperatorPolicyAWSは次のような管理ポリシーです。 OpenShift イメージレジストリオペレーターが Red Hat OpenShift Service on AWS (ROSA) クラスター内イメージレジストリで使用する Amazon S3 バケットとオブジェクトをプロビジョニングおよび管理して ROSA ストレージ要件を満たすことを許可します。 OpenShift イメージレジストリ Operator は Red Hat クラスターの内部レジストリーをインストールして管理します。 OpenShift

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAImageRegistryOperatorPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 27 日 20:13 UTC
- 編集時間:2023 年 12 月 12 日 19:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}/*"
      ]
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ROSAIngressOperatorPolicy

ROSAIngressOperatorPolicy は、OpenShift Ingress オペレーターが AWS (ROSA) クラスター上の Red Hat OpenShift Service のロードバランサーおよびドメインネームシステム (DNS) 設定をプロビジョニングおよび管理できるようにする AWS マネージドポリシーです。このポリシーでは、タグ値への読み取りアクセスを許可します。オペレーターは Route 53 リソースのためにこのタグ値にフィルター処理を行い、ホストゾーンを検出します。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAIngressOperatorPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 20 日 22:37 UTC
- 編集日時: 2023 年 4 月 20 日 22:37 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ROSAInstallerPolicy

ROSAInstallerPolicy は、Red Hat OpenShift Service on AWS (ROSA) インストーラが ROSA クラスターのインストールをサポートするAWSリソースを管理できるようにする AWSマネージドポリシーです。これには ROSA ワーカーノードのインスタンスプロファイルの管理が含まれます。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAInstallerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 6 月 6 日 21:00 UTC
- 編集日時： 2024 年 1 月 26 日 21:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ROSAKMSProviderPolicy

ROSAKMSProviderPolicy は、組み込みの ROSA AWS AWS 暗号化プロバイダーがキーマネジメントサービス (KMS) キーを管理して、AWSお客様が提供した KMS キーを使用した etcd データ暗号化をサポートできるようにする AWS マネージドポリシーです。このポリシーでは、KMS キーを使用してデータの暗号化および復号化ができます。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAKMSProviderPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 27 日 20:10 UTC
- 編集日時: 2023 年 4 月 27 日 20:10 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ROSAKubeControllerPolicy

`ROSAKubeControllerPolicy` は、ROSA Kubernetes コントローラーが ROSA クラスターの Amazon EC2、Elastic Load Balancing (ELB)、AWS キーマネジメントサービス (KMS) リソースを管理できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ROSAKubeControllerPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2023 年 4 月 27 日 20:09 UTC
- 編集日時: 2023 年 10 月 16 日 18:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ROSAManageSubscription

ROSAManageSubscription は、Red Hat OpenShift Service on AWS (ROSA) サブスクリプションの管理に必要な許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAManageSubscription をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2022 年 4 月 11 日 20:58 UTC
- 編集日時: 2023 年 8 月 4 日 19:59 UTC
- ARN: arn:aws:iam::aws:policy/ROSAManageSubscription

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ROSANodePoolManagementPolicy

ROSANodePoolManagementPolicy は、Red Hat OpenShift Service on AWS (ROSA) がクラスター EC2 インスタンスをワーカーノードとして管理することを許可する AWS マネージドポリシーです。これには、セキュリティグループを設定したり、インスタンスやボリュームにタグを付けたりする許可が含まれます。このポリシーにより、AWS キーマネジメントサービス (KMS) キーが提供するディスク暗号化による EC2 インスタンスの使用も許可されます。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSANodePoolManagementPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 6 月 8 日 20:48 UTC
- 編集日時: 2023 年 6 月 8 日 20:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ROSASRESupportPolicy

ROSASRESupportPolicy は、ROSA サイト信頼性エンジニアリング (SRE) に、ROSA クラスターノードの状態を変更する機能を含め、 AWS (ROSA) クラスター上の Red Hat OpenShift Service に関連するAWSリソースを最初に監視、診断、およびサポートするために必要なアクセス許可を提供する AWSマネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSASRESupportPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 6 月 1 日 14:36 UTC
- 編集日時： 2024 年 1 月 22 日 22:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ROSAWorkerInstancePolicy

ROSAWorkerInstancePolicy は、アカウント内の AWS (ROSA) ワーカーノード上の Red Hat OpenShift Service に Amazon EC2 インスタンスおよび AWS リージョン　コンピュートノードのライフサイクル管理への読み取り専用アクセスを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAWorkerInstancePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2023 年 4 月 20 日 22:35 UTC
- 編集日時: 2023 年 4 月 20 日 22:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

Route53RecoveryReadinessServiceRolePolicy

`Route53RecoveryReadinessServiceRolePolicy` は、Route 53 Recovery Readiness の サービスリンクロールポリシーである AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 7 月 15 日 16:06 UTC
- 編集日時: 2023 年 2 月 14 日 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

Route53ResolverServiceRolePolicy

`Route53ResolverServiceRolePolicy` は、Route53 Resolver が使用または管理する AWS のサービス またはリソースへのアクセスを可能にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 8 月 12 日 17:47 UTC
- 編集日時: 2020 年 8 月 12 日 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

S3StorageLensServiceRolePolicy

`S3StorageLensServiceRolePolicy` は、S3 Storage Lens が使用または管理する AWS のサービス およびリソースへのアクセスを可能にする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 18 日 18:15 UTC
- 編集日時: 2020 年 11 月 18 日 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

SecretsManagerReadWrite

`SecretsManagerReadWrite` は、経由で AWS Secrets Manager への読み取り/書き込みアクセスを提供する AWS マネージドポリシーです AWS Management Console。注: これは IAM アクションを除外するため、FullAccess ローテーション設定が必要な場合は を IAM と組み合わせてください。

このポリシーを使用すると

ユーザー、グループおよびロールに `SecretsManagerReadWrite` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 4 月 4 日 18:05 UTC
- 編集日時： 2024 年 2 月 22 日 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/SecretsManagerReadWrite`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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-*/*"
      ]
    }
  ]
}
```

詳細はこちら

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

SecurityAudit

SecurityAudit は、セキュリティ監査テンプレートがセキュリティ設定メタデータの読み取るためのアクセス付与に関する AWS マネージドポリシーです。AWS アカウント の設定を監査するソフトウェアに便利です。

このポリシーを使用すると

ユーザー、グループおよびロールに SecurityAudit をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集時間:2023 年 12 月 14 日 21:45 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v41 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  ]
}
```

詳細

- IAM アイデンティティセンターの AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

SecurityLakeServiceLinkedRole

SecurityLakeServiceLinkedRole は、Amazon Security Lake がユーザーに代わってサービス運用の許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 29 日 14:03 UTC
- 編集日時： 2024 年 2 月 29 日 19:14 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを決定します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- IAM ポリシーのバージョニングについて理解する
- AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する

ServerMigration_ServiceRole

`ServerMigration_ServiceRole` は、AWS Server Migration Service が VM を EC2 に移行する許可に関する AWS マネージドポリシーです。これにより、Server Migration Service が移行したリソースをお客様の EC2 アカウントに配置できるようにします。

このポリシーを使用すると

ユーザー、グループおよびロールに `ServerMigration_ServiceRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 8 月 11 日 20:41 UTC
- 編集日時: 2020 年 10 月 15 日 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*/*"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ServerMigrationConnector

`ServerMigrationConnector` は、AWS Server Migration Connector が VM を EC2 に移行できるように許可を付与する AWS マネージドポリシーです。AWS Server Migration Service との通信、ならびに「sms-b-」および「import-to-ec2-」で始まる S3 バケットへの読み取り/書き込みアクセスを許可します。さらに、サーバー移行コネクタのアップグレード、AWS Server Migration Connector アップグレードに使用されるバケット、AWS で AWS Server Migration Connector 登録、AWS へのメトリクスアップロードも許可します。

このポリシーを使用すると

ユーザー、グループおよびロールに `ServerMigrationConnector` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2016 年 10 月 24 日 21:45 UTC
- 編集日時: 2016 年 10 月 24 日 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationConnector`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ServerMigrationServiceConsoleFullAccess

`ServerMigrationServiceConsoleFullAccess` は、Server Migration Service Console のすべての機能を使用するために必要な許可に関する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ServerMigrationServiceConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2020 年 5 月 9 日 17:18 UTC
- 編集日時: 2020 年 7 月 20 日 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ServerMigrationServiceLaunchRole

ServerMigrationServiceLaunchRole は、移行したサーバーやアプリケーションを起動するため、AWS Server Migration Service が関連する AWS リソースを作成し、顧客の AWS アカウント に更新することを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに ServerMigrationServiceLaunchRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 11 月 26 日 19:53 UTC
- 編集日時: 2020 年 10 月 15 日 17:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ServerMigrationServiceRoleForInstanceValidation

`ServerMigrationServiceRoleForInstanceValidation` は、AWS SMS が使用済みデータ検証スクリプトを実行し、スクリプトの成功/失敗結果を SMS に送り返すことを許可する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ServerMigrationServiceRoleForInstanceValidation` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 7 月 20 日 22:25 UTC

- 編集日時: 2020 年 7 月 20 日 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ServiceQuotasFullAccess

`ServiceQuotasFullAccess` は、Service Quotas へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ServiceQuotasFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 6 月 24 日 15:44 UTC
- 編集日時: 2021 年 2 月 4 日 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ServiceQuotasReadOnlyAccess

`ServiceQuotasReadOnlyAccess` は、Service Quotas への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ServiceQuotasReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 6 月 24 日 15:31 UTC
- 編集日時: 2020 年 12 月 21 日 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
```

```
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ServiceQuotasServiceRolePolicy

`ServiceQuotasServiceRolePolicy` は、Service Quotas がユーザーに代わってサポートケースを作成できるようにする AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 5 月 22 日 20:44 UTC
- 編集日時: 2019 年 6 月 24 日 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

SimpleWorkflowFullAccess

`SimpleWorkflowFullAccess` は、Simple Workflow 設定サービスへのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `SimpleWorkflowFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/SimpleWorkflowFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

SupportUser

SupportUser は、AWS アカウント の問題のトラブルシューティングおよび解決を行う許可を付与する AWS マネージドポリシーです。このポリシーにより、ユーザーは AWS サポートに連絡してケースの作成および管理を行えるようにもなります。

このポリシーを使用すると

ユーザー、グループおよびロールに SupportUser をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:21 UTC
- 編集日時: 2023 年 8 月 25 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SupportUser`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

SystemAdministrator

SystemAdministrator は、アプリケーションおよび開発業務に不可欠なリソースに必要なフルアクセスを付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに SystemAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:23 UTC
- 編集日時: 2020 年 8 月 24 日 20:05 UTC
- ARN: arn:aws:iam::aws:policy/job-function/SystemAdministrator

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

TranslateFullAccess

`TranslateFullAccess` は、Amazon Translate へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `TranslateFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 27 日 23:36 UTC
- 編集日時: 2020 年 1 月 8 日 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

TranslateReadOnly

`TranslateReadOnly` は、Amazon Translate への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `TranslateReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2017 年 11 月 29 日 18:22 UTC
- 編集日時: 2023 年 5 月 24 日 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

ViewOnlyAccess

`ViewOnlyAccess` は、すべての AWS サービスのリソースおよび基本メタデータを閲覧する許可を付与する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `ViewOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:20 UTC
- 編集日時: 2023 年 3 月 6 日 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v17 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

VMImportExportRoleForAWSConnector

`VMImportExportRoleForAWSConnector` は、AWS コネクタを使用する顧客向け VM Import/Export サービスロールのデフォルトポリシーに関連する AWS マネージドポリシーです。VM Import/Export サービスはこのポリシーに基づいてロールを引き受け、AWS コネクタ仮想化アプライアンスから仮想化マシンの移行リクエストを満たします。(AWS コネクタは「AWSConnector」マネージドポリシーを使用して、顧客に代わって VM Import/Export サービスにリクエストを発行することにご注意ください) AMI および EBS スナップショットの作成、EBS スナップショットの属性の変

更、EC2 オブジェクトに「Describe*」呼び出しの実行、「import-to-ec2」で始まる S3 バケットからの読み取りを行えるようにします。

このポリシーを使用すると

ユーザー、グループおよびロールに VMImportExportRoleForAWSConnector をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 9 月 3 日 20:48 UTC
- 編集日時: 2015 年 9 月 3 日 20:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

VPCLatticeFullAccess

`VPCLatticeFullAccess` は、Amazon VPC Lattice へのフルアクセスを提供し、依存サービスへのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `VPCLatticeFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 3 月 30 日 02:49 UTC
- 編集日時: 2023 年 3 月 30 日 02:49 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
```

```
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

VPCLatticeReadOnlyAccess

VPCLatticeReadOnlyAccess は、AWS Management Console 経由で Amazon VPC Lattice への読み取り専用アクセスを提供し、依存サービスへの制限付きアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに VPCLatticeReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 3 月 30 日 02:47 UTC
- 編集日時: 2023 年 3 月 30 日 02:47 UTC
- ARN: arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

VPCLatticeServicesInvokeAccess

VPCLatticeServicesInvokeAccess は、Amazon VPC Lattice サービスを呼び出すためのアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに VPCLatticeServicesInvokeAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2023 年 3 月 30 日 02:45 UTC
- 編集日時: 2023 年 3 月 30 日 02:45 UTC
- ARN: arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

WAFLoggingServiceRolePolicy

`WAFLoggingServiceRolePolicy` は、SLR を作成してお客様のログを Firehose ストリームに書き込む AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 8 月 24 日 21:05 UTC
- 編集日時: 2018 年 8 月 24 日 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

WAFRegionalLoggingServiceRolePolicy

`WAFRegionalLoggingServiceRolePolicy` は、SLR を作成してお客様の口グを Firehose ストリームに書き込む AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 8 月 24 日 18:40 UTC
- 編集日時: 2018 年 8 月 24 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

WAFV2LoggingServiceRolePolicy

`WAFV2LoggingServiceRolePolicy` は、AWS WAF が Amazon Kinesis Data Firehose にログを書き込むことを許可するサービスにリンクされたロールを作成する AWS マネージドポリシーです。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 7 日 00:40 UTC
- 編集日時: 2020 年 7 月 23 日 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細

- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

WellArchitectedConsoleFullAccess

`WellArchitectedConsoleFullAccess` は、AWS Management Console 経由で AWS Well-Architected Tool へのフルアクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `WellArchitectedConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 29 日 18:19 UTC
- 編集日時: 2018 年 11 月 29 日 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

WellArchitectedConsoleReadOnlyAccess

`WellArchitectedConsoleReadOnlyAccess` は、AWS Management Console 経由で AWS Well-Architected Tool への読み取り専用アクセスを提供する AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに `WellArchitectedConsoleReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2018 年 11 月 29 日 18:21 UTC
- 編集日時: 2023 年 6 月 29 日 17:16 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

WorkLinkServiceRolePolicy

`WorkLinkServiceRolePolicy` は、Amazon WorkLink が使用または管理する AWS のサービス およびリソースへのアクセスをできるようにする AWS マネージドポリシーです。

このポリシーを使用すると

ユーザー、グループおよびロールに WorkLinkServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS マネージドポリシー
- 作成日時: 2019 年 1 月 23 日 19:03 UTC
- 編集日時: 2019 年 1 月 23 日 19:03 UTC
- ARN: arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを適用したユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、AWS はポリシーのデフォルトバージョンを確認し、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細

- IAM Identity Center の AWS マネージドポリシーを使用してアクセス許可セットを作成する
- IAM ID のアクセス許可の追加および削除
- IAM ポリシーのバージョニングについて理解する
- AWS マネージドポリシーの開始と最小特権のアクセス許可への移行

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。